IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

AMERICAN CIVIL LIBERTIES UNION, *et al.*,	)	
Plaintiffs,	)	Civil Action No. 98-CV-5591
v.	)	
ALBERTO R. GONZALES, in his official capacity as Attorney General of the United States,	)	
Defendant.	)	

DEFENDANT'S PROPOSED FINDINGS OF FACT
AND CONCLUSIONS OF LAW

Defendant respectfully submits, through counsel, the following proposed findings of fact and conclusions of law.

PROPOSED FINDINGS OF FACT

I. BACKGROUND

A. Findings Concerning Scope of Litigation

1. Defendant is Alberto R. Gonzales, the Attorney General of the United States, who is charged with enforcing the provisions of the Child Online Protection Act ("COPA") challenged in this action. (Stipulations at ¶ 1)

2. COPA was passed as part of the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub. L. No. 105-277, div. C, §§ 1401-06, 112 Stat. 2681, 2681-736 to 2681-741 (Oct. 21, 1998). The Act, codified at 47 U.S.C. §§ 230 & 231 (1998), was signed into law on October 21, 1998, with an effective date of November 20, 1998. This Court's temporary restraining order and subsequent entry of a preliminary injunction prevented COPA from going into effect on that date. *See Am. Civil Liberties Union v. Reno*, 31

F. Supp. 2d 473 (E.D. Pa. 1999). For ease of reference, citations to COPA herein will refer to its codification at 47 U.S.C. § 231.

3. Plaintiffs are either website operators, none of whom have anything to do with the commercial display and distribution of pornography on the Web, or associations suing on behalf of members who operate or access websites. (Am. Compl.)

B. Defining the Scope of COPA

4. COPA defines "material that is harmful to minors" as "any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind" that is "obscene" or that:

> (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;
>
> (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
>
> (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

47 U.S.C. § 231(e)(6). COPA defines a minor as "any person under 17 years of age." *Id.* at § 231(e)(7).

5. COPA's commercial purposes definition limits COPA's obligations to persons "engaged in the business" of distributing harmful-to-minors material. 47 U.S.C. § 231(e)(2)(A). Persons are "engaged in the business" only if they seek to profit from such material, and even businesses that seek to profit from harmful-to-minors material are not covered unless they do so

as a "regular course" of their business. *Id.* at § 231(e)(2)(B). COPA thus narrowly limits its obligations to businesses that regularly seek to profit from harmful material as a regular course of their business. By implication, an entity could not be prosecuted under COPA for the inadvertent, intermittent communication of material that the statute defines as harmful to minors.

6. These important qualifications reflect Congress's intent to target commercial pornography. Congress stated:

> Given that the scope of the bill is limited to commercial activity, and that the age verification system procedures prescribed under the bill represent standard procedures for conducting *commercial activity on pornographic web sites*, the effect of the bill is simply to reorder the process in such a way as to require age verification before pornography is made available, essentially requiring the *commercial pornographer* to put sexually explicit images "behind the counter." The *commercial pornographer* is not otherwise restricted in his trade.

H.R. Rep. No. 105-775, at 15 (1998) (emphasis added). *See also id.* at 7 ("While legitimate U.S. businesses should remain free from unnecessary government regulation, the adult entertainment industry has traditionally been subject to restrictions because of the dangers posed by pornographic material to children."). Not surprisingly, the House Report repeatedly refers to those covered by COPA variously as "publishers of pornography," "commercial purveyors of pornography," and "commercial sellers of material harmful to minors." *Id.* at 7, 14, 18.

C. <u>The Plaintiffs in This Litigation Are Not Within the Scope of COPA</u>

7. Plaintiffs represent a range of individuals and entities including speakers, content providers, and ordinary users on the World Wide Web (the "Web"), as that term is defined in the Act. Plaintiffs post content including, *inter alia*, resources on sexual health, safe sex, and sexual education; visual art and poetry; resources for gays and lesbians; online magazines and articles;

music; and books and information about books that are being offered for sale. (Stipulations at ¶ 2)

8. Some of the Plaintiffs provide interactive fora on their Web sites, such as online discussion groups, bulletin boards and chat rooms, which enable users to create their own material on Plaintiffs' Web sites. Some of the verbal and visual exchanges that could potentially occur in these chatrooms or in the postings on their bulletin boards may include language or images that contain sexual content. (Stipulations at ¶ 3)

9. None of the Plaintiffs is a commercial purveyor of what is commonly termed "pornography." (Plaintiffs' Testimony)

10. No Plaintiff has demonstrated that his or her business, or any part thereof, is devoted to making harmful-to-minors communications for profit. (Plaintiffs' Testimony)

11. No website Plaintiff has demonstrated that it intends to make harmful-to-minors communications for profit as a regular course of its business. (Plaintiffs' Testimony)

12. All of the Plaintiffs express a subjective fear of prosecution under the statute. (Stipulations at ¶ 30)

13. Although some or all of the Plaintiffs purport to fear prosecution under the statute, these fears are without a substantial basis in fact. (Plaintiffs' Testimony)

14. No Plaintiff has ever been contacted by state or local authorities, nor prosecuted nor arrested regarding any investigation into criminal violations. (Stipulations at ¶ 31)

15. The "speech" that Plaintiffs allege gives rise to their fear of prosecution does not contain any material that is designed to appeal or pander to a prurient (i.e., shameful, morbid, or obsessive) interest in sex. (Plaintiffs' Testimony; Def.'s Trial Ex. 282 at 8-9)

16. The "speech" that Plaintiffs allege gives rise to their fear of prosection does not contain any material that depicts, describes, or represents an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast, so as to come within the scope of COPA. (Def.'s Trial Exs. 279—280; Def.'s Trial Ex. 281 at 9-10)

17. All of the material that Plaintiffs allege gives rise to their fear of prosecution has literary, artistic, political, or scientific value for minors. (Def.'s Trial Exs. 279—280; Def.'s Trial Ex. D281 at 10-11)

18. Plaintiffs have had ample opportunity during discovery to offer objective facts and concrete examples to substantiate their fear of prosecution. (Pls.' Resp. to Def.'s Request for Docs. No. 13-15, Ex. 3 to Def.'s Mot. to Dismiss (Doc. No. 285))

19. To the extent Plaintiffs have identified Web-based chat, e-mail, bulletin board, or discussion group areas on their Web sites, they have failed to allege that they have knowledge of the information placed in these areas by users of their sites, so as to subject them to liability under COPA, 47 U.S.C. § 231(a)(7). (Plaintiffs' Testimony)

20. To the extent Plaintiffs have identified Web-based chat, e-mail, bulletin board, or discussion group areas on their Web sites, they have failed to allege that they actively take part in supervising and monitoring and filtering (i.e., selecting or altering) information placed in these areas by users of their sites, so as to subject them to liability under COPA. 47 U.S.C. § 231(b)(4). (Plaintiffs' Testimony)

21. Defendant incorporates by reference the disputed facts relating to Plaintiffs' standing set forth in the proposed pre-trial order filed on October 3, 2006. (Def.'s Disputed

Facts, pp. 72-84 (Doc. No. 319))

II. STATUS QUO: CHILDREN'S EXPOSURE TO PORNOGRAPHY ON THE WEB

A. The World Wide Web

22. The Web is a service that operates over the Internet. The Web is the complete set of documents residing on all Internet servers that use the Hypertext Transfer Protocol ("HTTP"), which is the protocol specifying how hypertext will be moved around the Web. (Mewett Testimony and Report ¶ 9)

23. The World Wide Web combines four basic components:

a. Hypertext, that is the ability, in a computer environment, to move from one part of a document to another, or from one document to another, through internal connections among these documents (called "hyperlinks" or "links");

b. Resource Identifiers, that is the ability, on a computer network, to locate a particular resource (computer, document or other resource) on the network through a unique identifier;

c. The Client-server model of computing, in which client software or a client computer makes requests of server software or a server computer that provides the client with resources or services, such as data or files; and

d. Markup language, in which characters or codes embedded in text indicate to a computer how to print or display the text, *e.g.* as in italics or bold type or font.

(Mewett Testimony and Report ¶ 10)

24. On the World Wide Web, a client program called a Web browser retrieves information resources, such as Web pages and other computer files, from Web servers using their network addresses and displays them, typically on a computer monitor, using a markup language that determines the details of the display. One can then follow hyperlinks in each page to other resources on the World Wide Web of information whose location is provided by these

hyperlinks. The act of following hyperlinks is frequently called "browsing" or "surfing" the Web. (Stipulations at ¶ 79)

25. Web pages are often arranged in collections of related material called "Web sites," which consist of one or more "Web pages." (Stipulations at ¶ 80)

26. To navigate to different pages on the Web, an HTTP request is sent to the Web server working at that IP address for the page required. In the case of a typical Web page, the HTML text, graphics and any other files that form a part of the page will be requested and returned to the client (the Web browser) in quick succession. The Web browser's job is then to render the page as described by the HTML and other files received, incorporating the images, links and other resources as necessary. This produces the on-screen "page" that the viewer sees. Most Web pages contain hyperlinks to other relevant and informative pages and perhaps to downloads, source documents, definitions and other Web resources. (Stipulations at ¶ 81)

27. When a viewer wants to access a Web page or other "resource" on the World Wide Web, he or she normally begins either by typing the Uniform Resource Locator ("URL") of the page into his or her Web browser, or by following a hypertext link to that page or resource. When the viewer does so, the server-name part of the URL is "resolved," or translated, into an Internet Protocol ("IP") address by the global, distributed Internet database known as the Domain Name System ("DNS"). This database stores all the registered domain names and associated IP addresses. When a user types in a domain name, the system looks it up and then uses for all remaining references the associated IP address that was found in the database. A Domain Name is the name that identifies one or more IP addresses on the Internet. The system allows people to refer to locations on the Internet by names, while the computers on the Internet

can communicate by referring to each other as numbers. The IP address is the numerical identifier for a computer or device on the Transmission Control Protocol/Internet Protocol ("TCP/IP") network. (Mewett Testimony and Report ¶ 12)

28. The U.S. Census Bureau's Current Population Survey's results show that in September 2001, approximately 54 percent of the U.S. population was using the Internet from any location. That figure rose to 59 percent in 2003. (Stipulations at ¶ 97)

29. The Internet is an interactive medium based on a decentralized network of computers. (Stipulations at ¶ 78)

30. The primary method of remote information retrieval over the Internet today is the World Wide Web ("WWW" or simply "the Web"). The Web is a global information space operating over the Internet, which people can read from and write to via a variety of different Internet-connected devices, including for example, computers, Personal Digital Assistants ("PDAs"), and cellular phones. (Mewett Testimony and Report ¶ 8)

31. Some Web sites serve as a proxy or intermediary between a user and another Web page. When using a proxy server, a user does not access the page from its original URL, but rather from a URL on the proxy server. (Stipulations at ¶ 82)

32. Some Web sites, in addition to displaying the page requested by the user, will also display content using "pop-up screens." These pop-ups open without prompting by the user. Pop-ups are most commonly used on commercial sites for advertisements, which may or may not be topically related to the content of the original Web site. (Mewett Testimony)

33. Some Web sites will automatically open new windows that a user did not affirmatively take steps to access, or will re-direct the user to a different site altogether. (Mewett Testimony)

34. Some content from the Internet is now capable of being viewed on devices other than traditional personal computers. Examples include mobile devices such as mobile phones, personal digital assistants ("PDAs") such as the Blackberry, portable audio/video players such as the iPod, and game consoles such as the XBox or PlayStation. (Stipulations at ¶ 96)

B. The Use of Search Engines on the Web

35. Modern search engines search for and index web pages individually. Search engines are web sites that provide links to relevant web pages, in response to search terms (words or phrases) entered by a user. They are a popular way of finding information online. (Stipulations at ¶ 83)

36. Most users interact with the Web by using a search engine. A search engine is a computer program designed to help find information stored on a computer system such as the World Wide Web. The search engine allows the user to request content that meets specific criteria (typically those containing a given word or phrase) and to retrieve a list of references that match those criteria. (Stipulations at ¶ 84)

37. The result of a Web search is usually a list of URLs with short explanatory summaries. Search engines do not search the Web; instead, they search regularly updated indexes to operate quickly and efficiently. (Mewett Testimony and Report ¶ 14)

38. Search engines obtain their Web page listings in two ways. Web site operators may submit their own Web pages to the search engines, or the search engines may "crawl" or

"spider" documents by following one hypertext link to another. The latter process returns the bulk of the Web pages and associated URL listings contained in search engine databases. Crawlers work by tracking and recording hypertext links in the Web pages that they index while crawling. A copy of each Web page visited is then stored on the search engine servers. These servers are generally located in server farms, and the major search engines may operate many thousands of these servers. When a user enters a query on a search engine via their browser, that query is sent to the databases on these servers. (Mewett Testimony and Report ¶¶ 19-20)

39. Search engines such as Google, MSN or Yahoo! Search, and directories such as Yahoo! Directory, give access to only a small part of the Web. This portion of the Web is often referred to as the Surface Web or the "Accessible" Web. The technology used by these conventional search engines does not provide access into a vast area of the Web called the Deep Web, which is much larger than the Surface Web. (Mewett Testimony and Report ¶ 16)

40. The Deep Web is composed of Web documents that are poorly indexed or not indexed at all by the broad-based conventional search engines. Pages on the Deep Web comprise a variety of materials, including dynamic content, databases, documents omitted because they are too large, pages protected by the author, and pages with restricted access. (Mewett Testimony and Report ¶¶ 21, 23)

41. Most users of the Internet who start their typical surfing journey using a search engine will initially view the Surface Web. However, once links start to be clicked and the journey progresses, the likelihood of staying in the Surface Web diminishes. (Mewett Testimony and Report ¶ 24)

42. It is becoming more likely that users of the Internet will be steered to content in the Deep Web, for several reasons. Web content providers increasingly use dynamic content in their Web sites. In addition, some Web content providers use URL redirection to steer viewers from the URL that they intended to access to a different URL. Redirected content frequently is found in the much larger, less structured Deep Web. (Mewett Testimony and Report ¶ 25)

43. It is not possible to determine precisely the number of Web pages in either the Surface Web or the Deep Web. The Surface Web has been reasonably estimated to be anywhere between 25 billion and 64 billion pages in size as of 2005, with an estimated 50 million pages being modified or added every day. The Deep Web has been estimated to be over 500 times larger than the Surface Web. (Mewett Testimony and Report ¶¶ 17, 31)

C. The Use of HTTP Protocol on the Web

44. HTTP stands for hypertext transfer protocol; it is widely used on the Internet. (Stipulations at ¶ 110)

45. FTP stands for file transfer protocol. It is used primarily to transfer files across the Internet. (Stipulations at ¶ 109)

46. Among the web sites that use primarily HTTP are *The New York Times, Washington Post,* and even plaintiffs ACLU, Electronic Frontier Foundation, Electronic Privacy Information Center, and Salon Media Group. (Stipulations at ¶ 112)

47. Most URLs use HTTP. (Stipulations at ¶ 113)

48. There are forms of content on the World Wide Web, such as streaming video, that do not use the HTTP protocol. However, this content is found within larger Web pages that use

the HTTP protocol. Further, a viewer can publicly access these forms of content over the Internet through the use of HTTP. (Mewett Testimony)

49. Numerous practical and technical obstacles will prevent a wholesale shift of websites from HTTP to FTP. Search engines are structured around HTTP, consumer search habits are deeply ingrained, and firewalls retard movement from HTTP pages to FTP pages because the protocols operate from different ports. Even if some future shift from HTTP to FTP were to occur, websites are likely to maintain some usage of HTTP. (Mewett Testimony)

50. It is technically possible to convert a web site delivered over the HTTP protocol to the FTP protocol. However, it is unlikely that all of the existing code on the site would work without modification. This is particularly true if the web page has embedded CGI scripts, which are the most common way for Web servers and Web browsers to handle information from HTML forms on Web pages. (Mewett Testimony and Rebuttal Report ¶ 25)

51. A web site operator who wishes to convert his site from HTTP to FTP would likely need to maintain at least some of the pages on the web site in HTTP, with traffic moving between the HTTP pages and the FTP pages. (Mewett Testimony and Rebuttal Report ¶ 25)

52. There may be complications for the viewer if a web site is converted to FTP. FTP requires specific ports, ports 20 and 21, to be left open to facilitate the connection. Some work environments, and even firewalls in domestic environments, may have these ports closed, rendering the web site inaccessible. In addition, firewalls may time out during large data transfers from FTP sites, causing an error to be generated. (Mewett Testimony and Rebuttal Report ¶ 25)

53. It would be important for a web site operator to ensure that the viewer of his site

does not need to learn new Internet browsing skills to access his site. It is likely, however, that the conversion of a web site to FTP would require the viewer to reconfigure a firewall to confirm that the necessary ports are open for FTP. In addition, the viewer would need to change to a convention of typing "FTP://" in a browser bar, which would likely create confusion as browsers currently assume that a viewer intends to access HTTP and will automatically insert "HTTP://" in front of a domain name that is entered into a browser bar. (Mewett Testimony and Rebuttal Report ¶ 26)

54. Search engines index only HTTP sites, and so simply entering a search term in the search engine will not return an FTP site. A viewer would either need to know the exact address of an FTP site to access it, or the web site operator would be required to maintain an HTTP site to direct viewers to the new site. (Mewett Testimony and Rebuttal Report ¶ 27)

55. Security concerns would likely deter website operators from converting to FTP. That protocol is not designed for sharing sensitive information, such as payment transactions or other financial information. It is therefore likely that a commercial website operator who operates an FTP site would revert to the HTTP protocol for the purpose of processing sensitive information, rather than converting the web site entirely to FTP. (Mewett Testimony and Rebuttal Report ¶ 28)

D. The Prevalence of Sexually Explicit Content on the Web

56. Paul Mewett of CRA International, Inc., and Dr. Philip B. Stark, Ph.D., performed a study of sexually explicit material on the World Wide Web on behalf of Defendant. For the purpose of this study, several samples of URLs were drawn. First, a random sample was drawn of the URLs available in the index maintained by Google Inc. for its search engine, and another

random sample was drawn of the URLs available in the index maintained by the Microsoft Corporation for its MSN search engine. Second, a random sample was drawn of actual queries entered into the MSN, Yahoo!, and AOL search engines, and the URLs returned by the search engines from the queries in that sample were studied. Third, a study was performed of URLs returned by search engines from the most popular queries, as recorded by Wordtracker. (Wordtracker is a service that collects queries from several search engine aggregators.) (Mewett and Stark Testimony)

57. Approximately 1.1 percent of the Web pages in both the Google and MSN indexes are sexually explicit. Given the estimates of the size of the Surface Web, it is reasonable to estimate that between 275 million and 704 million of the Web pages on the Surface Web alone are sexually explicit. (Stark Testimony and Report ¶ 10; Mewett Testimony and Report ¶¶ 31, 71)

58. In addition, sexually explicit Web pages are returned more frequently in response to search engine queries than are other Web pages. Approximately 1.7 percent of the URLs returned from the search engine query data set from MSN, Yahoo!, and AOL are sexually explicit. Approximately 6 percent of the queries in that data set return at least one sexually explicit Web page in response to the query. (Stark Testimony)

59. Sexually explicit Web pages are returned significantly more frequently in response to the most popular search engine queries. Approximately 14.1 percent of the URLs returned in response to the search engine query data set from Wordtracker are sexually explicit. Approximately 37.1 percent of the queries in that data set return at least one sexually explicit Web page in response to the query. (Stark Testimony)

60. Even seemingly innocent popular queries will return sexually explicit material. An examination of the data set from Wordtracker reveals that innocuous queries such as "Online Games" and "Oops" return sexually explicit material. (Mewett Testimony and Report ¶ 57; Allen and Finkelhor Testimony)

61. Envisional, a company that operates a search facility for companies that can detect online misrepresentations of their brands, performed a study on children's toy brands. Its search of the 26 most popular children's characters, including Pokemon, My Little Pony, Toy Story and Furby, revealed several thousand links to pornographic sites. Thirty percent of these sites featured hard core sexually explicit material. The remainder of those linked sites contained nudity, obscene language or extreme violence. (Mewett Testimony and Report ¶ 57)

62. In 2000 a web survey found that keyword searches of "sex education," "sexual health," and "sex advice for teens" yielded 1,556 web pages, of which 63 percent were pornographic. (Def.'s Trial Ex. 274)

63. Of the sexually explicit Web pages in the Google index, approximately 44.2 percent are domestic, that is, are hosted in the United States. Of the sexually explicit Web pages in the MSN index, approximately 56.7 percent are domestic. (Stark Testimony and Report ¶ 10)

64. Domestic sexually explicit sites appear to be especially popular in comparison to foreign sexually explicit sites. Of the sexually explicit Web pages in the set of URLs returned from the sample set of search engine queries, approximately 88.4 percent are domestic. Similarly, of the sexually explicit Web pages in the set of URLs returned from the Wordtracker set of the most popular queries, approximately 87.4 percent are domestic. (Stark Testimony)

65. The majority of sexually explicit websites are commercially driven. The sexually

explicit websites can be categorized into two groups – "feeder" websites, and membership websites or "pay sites." (Zook Testimony and Report at 3-4)

66. Membership sexually explicit websites use feeder websites as "bait" for the pay sites, and the feeder websites make their money by successfully guiding viewers to premium services on other websites. (Zook Testimony and Report at 4)

67. Affiliate fees from the membership websites are the primary source of revenue for feeder sexually explicit websites. (Zook Testimony)

68. Feeder adult websites offer pictures amidst a maze of banners and pop-up windows that direct visitors to membership websites. (Zook Testimony and Report at 4)

69. Because of large bandwidth requirements, companies specializing in the adult industry, rather than traditional hosting services, generally host adult websites. Because traffic to adult websites can build quickly, hosting is generally the most significant cost to websites. (Zook Testimony and Report at 5)

70. These hosting costs make the paid membership websites essential to the functioning of a commercial Internet adult industry. The more content that is downloaded from a website, the higher consumption of bandwidth. Without paid memberships, the Internet adult industry could not pay for the bandwidth that it consumes. (Zook Testimony and Report at 5)

71. According to an article published in 2003 by Matthew Zook, approximately 85 percent all adult membership websites are hosted in the United States. Of all feeder adult websites, 93.3 percent are hosted in the United States. (Zook Testimony)

72. Membership adult websites would face some barriers in relocating outside of the United States, as it would be more difficult to process credit card fees, to generate new content,

or to manage memberships. (Zook Testimony)

E. Children's Exposure to Sexually Explicit Content on the Web

73. The World Wide Web is widely accessible by minors. According to a recent study conducted on behalf of the U.S. Department of Education, approximately 59 percent of all students (from nursery school through the 12th grade) use the Internet. Twenty-three percent of students in nursery school use the Internet, as do 32 percent of students in kindergarten, 50 percent of students in the 1st through 5th grades, 70 percent of students in the 6th through 8th grades, and 79 percent of students in the 9th through 12th grades. (Def.'s Trial Ex. 81)

74. In light of the widespread availability of the Internet, a parent cannot guarantee that his or her child will not have access to sexually explicit material, even if he or she were to take the drastic step of removing computers from the home. In addition to using the Internet in their own homes, 43 percent of all students use the Internet at school, 10 percent use the Internet at libraries, and nine percent use the Internet at other person's homes. (Def.'s Trial Ex. 81 at 25)

75. Minors commonly are exposed to pornography on the Internet. One report has found that 25% of minors surveyed between the ages of 10 and 17 who regularly use the Internet inadvertently viewed pornography in the prior year. That number jumps to 70% when focusing on minors between the ages of 15 and 17. (Pls.' Trial Ex. 54 at 132-33 [hereinafter "NRC Report"])

76. Children are becoming exposed more frequently to sexually explicit material on the Internet. In 1999, Dr. Finkelhor conducted the first Online Victimization of Youth study ("YISS-1"). The study found, inter alia, that at the time of the interviews one-third of parents and guardians of the youths had filtering or blocking software on the youths' computers at home.

(Def.'s Trial Ex. 1 at ix; Finkelhor and Allen Testimony)

77. YISS-1 found also that one-quarter of the interviewed youths had in the past year been exposed to unwanted sexual material while using the Internet at home. (Def.'s Trial Ex. 1 at ix; Finkelhor and Allen Testimony)

78. Dr. Finkelhor conducted a second study in 2005, the Online Victimization of Youth study ("YISS-2"). The results of YISS-2 were released on August 9, 2006. (Def.'s Trial Ex. 2; Finkelhor and Allen Testimony)

79. The second study shows that, despite a reported increase in filter use, the rate of unwanted sexual material reaching 10-17 year-olds has risen. (Def.'s Trial Ex. 2 at 1; Finkelhor and Allen Testimony)

80. The 2005 study noted that the increase in youths' exposure to unwanted sexual material occurred after the enactment of 18 U.S.C. § 2252B in 2003, which made it a criminal offense to use a misleading domain name on the Internet with the intent of deceiving a minor into viewing harmful sexual material. (Def.'s Trial Ex. 2 at 8 n.8; Finkelhor and Allen Testimony)

81. The 2005 study also reported a larger proportion of exposure incidents happened when youths were "surfing" the Web - 83 percent (YISS-2) compared to 71 percent (YISS-1). More than one-third of surfing exposure incidents happened when youths were doing online searches (40 percent), clicking on other links in other web sites led to 17 percent of exposures, misspelled web addresses led to 12 percent, and 14 percent were from pop-up ads. In YISS-2, 18 percent of youth with unwanted exposures while surfing online said they were brought to another sex site when they tried exiting the first site they were in. (Def.'s Trial Ex. 2 at 9, 30,

32, 36; Finkelhor and Allen Testimony)

82. The 2005 survey found that, inter alia, exposure incidents that were very or extremely upsetting to youths–distressing exposures--had increased from 6 percent in YISS-1 to 9 percent in YISS-2. (Def.'s Trial Ex. 2 at 9; Finkelhor and Allen Testimony)

83. Minors who can read and type are capable of conducting Web searches as easily as operating a television remote. While a four-year-old may not be as capable as a thirteen-year-old, given the right tools (*e.g.*, a mouse and browser software) each has the ability to "surf" the Web and will likely be exposed to harmful material. (H.R. Rep. No. 105-775, at 9-10 (1998)) (Allen Testimony)

84. Even a child supervised by the best-informed and perceptive adult may be exposed to pornography by accidentally mistyping a website's address or by searching for common terms. Many websites do not warn viewers of their harmful material prior to displaying it, setting a trap for even experienced Web surfers. (H.R. REP. NO. 105-775, at 10 (1998)) (Finkelhor, Stark, and Mewett Testimony)

85. Even the most persistent parent cannot prevent a determined child from viewing harmful material. Children can view harmful material when adults are absent or not paying attention. (Allen, Finkelhor, and Eisenach Testimony)

86. In the "bricks and mortar" world, stores and enterprises that offer adult entertainment (e.g., video stores), often segregate the "adult" material for sale in their establishments by creating a separate room or section of their establishment with signs designating "Adult area," with no one under a certain specified age permitted to enter. In the case of establishments selling adult magazines, special efforts are made to display adult

magazines in a separate rack or area of the store, behind the counter, or behind special blinder racks, for the purpose of compliance with various state "harmful to minors" statutes including "display" laws. (H.R. Rep. No. 105-775, at 11)

87. By contrast, purveyors of sexually explicit material on the World Wide Web generally display many unrestricted and sexually explicit images to advertise and entice the consumer into engaging in a commercial transaction. (H.R. Rep. No. 105-775, at 10.)

88. Many of the numerous adult sites on the World Wide Web openly allow children under the age of 17 to see hard-core and soft-core pornography pictures for free by simply clicking on any link to an adult pornography site's home Web page. (H.R. Rep. No. 105-775, at 10)

89. Such pictures are listed under various types of banner or titles, including "Previews," "Teasers," "Guests," "Free Samples," "Free Pictures," which when clicked on will allow the visitor to see short clips or outtakes of X-rated movies, including amateur and "home" movies. (H.R. Rep. No. 105-775, at 10)

90. Pornography sites are sometimes "mousetrapped" or programmed to make them difficult to exit. Clicking an exit button takes viewers into another sexually explicit site instead of allowing them to leave. (H.R. Rep. No. 105-775, at 10; Finkelhor, Allen, and Mewett Testimony)

91. Even if the drastic step of ridding the household of computers were taken, minors still will have access to harmful material from computers with Internet connections located in schools, libraries, retail outlets, and other people's homes, as well as Internet access over cell phones, personal digital assistants, and other electronic media. (Finkelhor and Mewett

Testimony)

92. According to the NRC report, "it is probably not feasible [for parents] to provide constant supervision of [a] child's Internet access, especially as [the] child gets older." (Pls.' Trial Ex. 54 at 223)

93. The NRC report concludes that, while parental supervision and education may be useful in part to counter the problem of minors' exposure to sexual materials on the Internet, "the expectations for such education and socialization should not be unrealistic." (Pls.' Trial Ex. 54 at 371)

F. Exposure to Pornography on the Web Has Harmful Effects on Children

94. The exposure to pornography has harmful effects on minors. (Allen and Finkelhor Testimony)

95. Over the past four decades, new technologies have made sexually explicit content more widely available, especially to children, while the content of this pornography has become more graphic and extreme. (Def.'s Trial Ex. 274)

96. The pornography industry is large and profitable. The adult entertainment industry was projected to earn $12.6 billion in 2005. (Def.'s Trial Ex. 274)

97. Extensive social science research over the past 20 years has shown that watching pornography negatively impacts our attitudes, beliefs, and values about sex, intimacy, and family. It engenders sexual callousness, fosters the idea that women are subservient to men, decreases belief in honesty and trust between intimate partners, and trivializes sexual assault and abuse. It results in a loss of respect for female sexual autonomy and lowers the inhibition of men to be aggressive towards women. (Def.'s Trial Ex. 274)

III. FILTERING SOFTWARE OFFERS AN INADEQUATE SOLUTION TO THE PROBLEM

A. Overview

98. Internet content filtering software cannot completely protect minors from exposure to sexually explicit material on the World Wide Web. The status quo solution—filtering software without any government regulation—fails to protect children adequately. (Finkelhor, Allen, Mewett, Eisenach, and Neale Testimony)

99. Filtering software tends to underblock sexually explicit material. Thus, minors will be exposed to sexually explicit material on the World Wide Web even if filtering software is used. (Finkelhor, Allen, Mewett, Eisenach, and Neale Testimony)

100. Filtering software also tends to overblock non-sexually explicit material. Software that is more effective at avoiding the underblocking of sexually explicit material also tends to be less effective at avoiding the overblocking of sexually explicit material. Thus, in the absence of the solution offered by COPA, parents are left with the Hobson's choice of allowing their children to be exposed to sexually explicit material or of cutting off their children's access to a significant portion of other materials on the World Wide Web. (Finkelhor, Allen, Mewett, Eisenach, and Neale Testimony)

101. The use of filtering software requires technological sophistication, money, and monitoring, but, most importantly, offers no assurance that the product will work effectively. (Mewett and Eisenach Testimony)

102. The defects in filtering software are inherent. Filtering software relies largely or entirely on the parsing of text, but that parsing will never perfectly distinguish sexually explicit

material from non-sexually explicit material. (Neale Testimony)

103. There is a market defect that ensures that filtering software will not improve substantially. Producers of residential filtering products lack an incentive to seek to improve these products. (Eisenach Testimony)

B. The Architecture of Filtering Software

104. Internet content filtering software attempts to block certain categories of material that a Web browser is capable of displaying, including "adult" material. Filters categorize Web sites or pages based on their content. By classifying a site or page, and refusing to display it on the user's computer screen, filters can be used to prevent children from seeing material that might be considered unsuitable. In addition, businesses often use filters to prevent employees from accessing Internet resources that are either not work related or otherwise deemed inappropriate. (Stipulations at ¶ 85)

105. Some Internet content filters can be purchased on a CD or downloaded from the Internet and installed on a personal computer. Some filters are designed to be run on a server in a corporate, library, or school environment. Other filters are built into the services provided by Internet Service Providers. (Stipulations at ¶ 86)

106. Residential PC-based Internet content filtering programs generally work by installing themselves between the application layer (such as the browser) and the protocol layer (the mechanism for transporting data across computer networks). The software then acts as a conduit between the browser and the Web server, where it intercepts outbound requests and inbound data in order to filter them. (Mewett Testimony and Report ¶ 33; Neale Testimony and Report, ¶ 4.3)

107. Corporate and educational Internet content filtering products, commonly referred to as enterprise filters, are marketed for and designed to be implemented in a different environment than residential Internet content filtering products. (Eisenach Testimony and Rebuttal Report ¶¶ 26, 27)

108. Internet content filters use two main approaches, normally in tandem. The first approach uses a "black list" of known Web sites, areas within Web sites, or specific Web pages. Outbound requests are checked against this list, and the software attempts to block the requested material if it matches the list. (Mewett Testimony and Report ¶ 34; *see* Stipulations ¶¶ 87-88)

109. The second approach involves "dynamic filtering," *i.e.*, the checking of inbound data against keywords and/or phrases in an attempt to establish if that data contains content that contravenes the filtering rules. If it does, then the software attempts to block the data. Internet content filtering companies use a variety of proprietary algorithms to achieve this process. In essence, however, they all attempt to achieve the same result---determining whether there are sufficient words, or a particular usage of words, to justify blocking the page. Text filtering at this stage can take place in either the URL itself (*i.e.*, does a particular term exist within the URL), within the text on the page or source code associated with the page, or finally in the links on the page to other pages within the site or other sites. (Mewett Testimony and Report ¶ 34; Neale Testimony and Report, ¶ 3.3.1 – 5)

110. Some filtering programs can be used by parents to prevent their children from having any access to parts of the Internet other than the Web, and to certain Internet applications which parents do not want their children to have any access to, such as e-mail, chat, instant messaging, newsgroups, message boards, and peer-to-peer file sharing. (Stipulations at ¶ 95)

111. A filter that allows access only to Web sites that have been thoroughly checked and found to contain no content in a certain category is called a "white list." (Stipulations at ¶ 89)

112. Some filters also use "white lists" of content that should never be blocked. White lists are lists of URLs or IP addresses that the filtering company has determined do not point to any content their filter is designed to block. A very restrictive filter might block all URLs except those included on a white list. (Stipulations at ¶ 90)

113. In addition to relying on black lists and white lists, some filters also use "key words" or other "dynamic filtering" techniques to attempt to limit access to certain Web pages. Filtering companies may compile lists of words and phrases associated with content that should be blocked, even if the page has not previously been categorized. Some products just attempt to remove those words from the page, while others attempt to block the entire Web page that contains these words or phrases. (Stipulations at ¶ 92)

114. A filter that responds solely to the text making up the name of an image file (*e.g.*, blowjob03.jpg) is a text-based filter, not an image-based filter. Similarly, filters that respond solely to the text making up the names of audio files (*e.g.*, screamingorgasm.mp3) or video files (*e.g.*, blowjobs.jpeg) are text-based filters (not audio-based or video-based filters). (Stipulations at ¶ 93)

115. No commercially available filtering product uses image filtering. (Neale Testimony)

116. The task of keeping an up-to-date "black list" is mammoth. After entries have been initially categorized, they need to be regularly rechecked to confirm that the site has not

changed its content, and therefore is in need of re-categorization. As new domains continue to become available, the number of possible domains that must be analyzed for possible inclusion in a "black list" grows too. This increase forces a major dependency on the real-time analysis technology being employed to evaluate the page. For example, a survey in April 2006 by the company Netcraft identified in excess of 80 million domains in use world wide. (Neale Testimony and Mewett Testimony and Report ¶ 35)

117. The sheer size of the Web means only a very small (and shrinking) proportion of existing Web pages and Web sites can be classified by hand (*i.e.*, on the basis of subjective decisions made by human reviewers); so the overall effectiveness of a filter will always be a function of the performance of its automated classification software. (Mewett and Neale Testimony)

118. Some filters allow the user to block only certain categories, such as pornography and adult/sexually oriented materials; other filters do not allow for customization, but rather the user must select a predefined list of settings relating to a level of filtering or an appropriate age range. (Mewett Testimony and Report ¶ 39)

119. Alternative Internet access devices ("IADs") are rapidly penetrating the population of both adults and children. The Center for the Digital Future reports that 14.5 percent of those surveyed in 2003 reported accessing the Internet through a cell phone, wireless personal digital assistant ("PDA") or wireless computer, up from 9.2 percent in 2002. (Eisenach Testimony and Principal Report ¶ 44)

120. Many cell phones now include the ability to browse the Web, and adult content providers are actively pursuing this market as an outlet for their materials. (Mewett Testimony and Report ¶ 76)

121. Any filtering software for mobile phones cannot be more effective, and likely will be significantly less effective, than filtering software for personal computers. Because a mobile phone has limited bandwidth and memory, the software cannot be installed on the device and thus must be resident only on the server. Filtering software that resides only on a server will face significant defects in its effectiveness. (Mewett Testimony)

122. Traditional web pages are around 20K in size. Webpages designed for mobile phones average 1K to 2K in size because they are designed specifically for display on mobile phone screens and other portable devices. These mobile phone web pages are particularly difficult to classify accurately, because these smaller pages have fewer features that can be used to differentiate content. Consequently, problems with feature-driven classification are magnified in the classification of web pages for mobile phones. (Mewett and Neale Testimony)

123. Any attempt to filter mobile-optimated web pages will be forced to rely on an attempt to filter images. The technology for image filtering is deficient. (Mewett and Neale Testimony)

C. The (In)Effectiveness of Filtering Software

124. Internet content filtering software may be ineffective in two ways: underblocking and overblocking. Underblocking occurs when the filter fails to block content that would meet the filtering criteria (such as sexually explicit content). Overblocking occurs when the filter prevents access to material that does not meet the filtering criteria, resulting in the

inaccurate blocking of, for example, political, social, and health-related Web sites. (Mewett Testimony and Report ¶ 37)

125. Difficulties both with underblocking and with overblocking have led some parents to become dissatisfied with filtering software, and have led them to discontinue the use of that software. According to a survey conducted by one major Internet service provider, one in five former users of parental controls reported that the reason they ceased using such controls is that they did not believe that these controls were effective. According to the same study, some parents have reported that they disabled their filters because their children could not access Web sites needed in order to do their homework. (Mewett Testimony and Report ¶ 37)

126. ContentProtect, CyberPatrol, CyberSitter, McAfee, NetNanny, and Norton were rated by TopTenReviews in the 2006 Internet filter review as among the best content filters on the market. (Mewett Testimony and Report ¶ 38)

127. Mr. Mewett performed tests of these filters, as well as filters offered by AOL and MSN, two internet service providers that offer a nationwide product. (Mewett Testimony and Report ¶ 38)

128. Several of the filter products offer a range of settings to specify the type of material that the user hopes to block and not to block. In his tests, Mr. Mewett set the filter products at the settings that appeared to be the most likely to block sexually explicit material without blocking non-sexually explicit material. He also tested the filters at their default settings where applicable. (Mewett Testimony and Report ¶ 39)

129. Mr. Mewett tested the filters against data sets of URLs, described above, consisting of random samples drawn from the Google and MSN search engine indices; URLs

returned in response to a random set of searches on the MSN, Yahoo!, and AOL search engines; and URLs returned in response to the most popular searches as reported by the Wordtracker service. (Mewett Testimony and Report ¶ 50)

130. Mr. Mewett classified the URLs he tested into several categories. One category was for web pages with no sexual content. This first category of web pages was tested to determine the frequency at which the filter products block non-sexually explicit web pages. A second category was for sexually explicit web pages for which the apparent primary purpose was only adult entertainment. Web pages with a different apparent primary purpose, such as an education, literary, or health-related purpose, were not included in this category. This second category of web pages was tested to determine the frequency at which the filter products fail to block sexually explicit web pages. (Mewett Testimony and Report ¶¶ 58, 63)

131. Dr. Stark performed a statistical analysis of the results of this testing. With regard to the sets of web pages drawn from the Google and MSN search engine indices, Dr. Stark's analysis found that the various filter products failed to block the sexually explicit web pages from 8.6 percent to 60.2 percent of the time. The various filter products blocked the non-sexually explicit web pages from 0.4 percent to 23.6 percent of the time. As a general rule, the more that a particular filtering product overblocked, the less that it underblocked, and vice versa. None of the products had a combined underblocking and overblocking score that was less than 16.3 percent. (Stark Testimony and Report ¶ 11)

132. With regard to the web pages that were returned from a random sample of queries on the MSN, Yahoo!, and AOL search engines, Dr. Stark's analysis found that the various filter products failed to block the sexually explicit web pages from 6.2 percent to 43.4

percent of the time. The various filter products blocked the non-sexually explicit web pages from 0 percent to 20.7 percent of the time. Again, as a general rule, the more that a particular filtering product overblocked, the less that it underblocked, and vice versa. None of the products had a combined underblocking and overblocking score that was less than 15.3 percent. (The two products with a 0 percent overblocking score also underblocked sexually explicit web pages at rates of 20.4 percent and 43.4 percent, respectively.) Among the queries that retrieved at least one sexually explicit web page, between 15.6 percent and 56.1 percent of those queries retrieved at least one sexually explicit web page that was not blocked by the various filters. (Stark Testimony and Report ¶ 11)

133. With regard to the web pages that were returned from the most popular queries as reported by Wordtracker, Dr. Stark's analysis found that the various filter products failed to block the sexually explicit web pages from 1.3 percent to 12.6 percent of the time. The various filter products blocked the non-sexually explicit web pages from 2.9 percent to 32.8 percent of the time. Again, as a general rule, the more that a particular filtering product overblocked, the less that it underblocked, and vice versa. None of the products had a combined underblocking and overblocking score that was less than 13.1 percent. (Stark Testimony and Report ¶ 11)

134. These estimates likely understate the prevalence of sexually explicit web pages and the rates at which filters fail to block sexually explicit web pages or block non-sexually explicit web pages. For example, Dr. Stark counted queries that did not retrieve any working websites in the denominator of estimates of the prevalence of sexually explicit material. Further, the definition of a sexually explicit web page that was used for the purpose of Mr. Mewett's and Dr. Stark's study is restrictive; in order to qualify, the page must have sexually explicit content

that is clearly adult entertainment, and that content must be visible without clicking anything, not even the "play" button of a video. Similarly, the definition of a non-sexually explicit web page that was used for the purpose of this study is also restrictive; in order to qualify, the page must have no nudity or sexual content whatsoever. (Stark Testimony and Report ¶ 20; Mewett Testimony and Report ¶ 63)

135. The Plaintiffs retained J. Christopher Racich of First Advantage to perform a study of the effectiveness of Internet content filtering software. He tested four filtering products, but only submitted expert reports with respect to two of those products. He tested each of those products with respect to their efficacy at blocking sexually explicit material, but he did not test those products in any way with respect to their efficacy in avoiding the blocking of non-sexually explicit material. (Racich Testimony)

136. Mr. Racich tested the Safe Eyes 2006 brand of filtering software, and set that product to attempt to block all of its default categories, including "nudity," "pornography," "sex," and "tasteless/gross," and also to attempt to block the additional categories of "adult" and "lingerie." (Racich Testimony)

137. Mr. Racich tested the 8e6 Home Internet Protection Services brand of filtering software, and set that product to attempt to block all of its default categories, including "obscene," and "r-rated." (Racich Testimony)

138. In Mr. Racich's tests, the filters failed to block many sexually explicit Web pages. (Racich Testimony and Def.'s Trial Exs. 386-87)

139. Although Mr. Racich did not disclose these additional tests in his expert reports, he also tested the CyberPatrol filtering software (at both its "mature teen" and "young teen"

settings) and the Net Nanny filtering software. In those tests, the Cyber Patrol software failed to block 304 out of 1267 sexually explicit web pages (as identified in Mr. Mewett's study) at its "mature teen" setting, and failed to block 284 out of 1264 sexually explicit web pages at its "young teen" setting. The Net Nanny software failed to block 311 out of 1265 sexually explicit web pages in Mr. Racich's test. (Racich Testimony)

140. The Mewett study confirms that even popular and well-reviewed filtering products perform poorly. Filters that have significant portions of market share, and filters that have been rated highly by reviewers, in fact performed particularly poorly. (Mewett and Stark Testimony)

141. Filters do not necessarily block a certain URL every time that that URL is entered into a browser. In other words, a claimed success rate of 80 percent in blocking sexually explicit content does not entail that 80 percent of all content is always blocked; instead, the same content may be blocked 80 percent of the time and allowed 20 percent of the time. (Mewett Testimony and Report ¶ 74)

142. This study also confirms that there is a direct relationship between underblocking and overblocking. Filtering products achieve lower rates of underblocking only by blocking significantly more "clean" content. (Mewett and Stark Testimony)

143. Overblocking is a significant concern. Because non-sexually explicit web pages were significantly greater in number in Mr. Mewett's and Dr. Stark's study than were sexually explicit web pages, even a relatively small increase in the percentage of "clean" web pages that are blocked can result in many blocked pages for a typical user. (Mewett and Stark Testimony)

144. Examples of non-sexually explicit web pages that were blocked by the filters tested by Mr. Mewett include the following: www.nakedjuice.com (a fruit juice company); www.topless-sandal.com (a footwear company); www.boobiethon.com (a breast cancer awareness web site); www.aclufl.org/news_events/calendar/index.cfm?viewDate=6%2F1%2F2005 (the calendar of a state ACLU chapter); www.cia.gov/cia/publications/factbook/geos/mx.html (the CIA World Fact Book); www.i-love-cats.com; and www.weightlossguide.com. (Mewett Testimony and Report ¶ 80 and Rebuttal Report ¶ 12)

145. Even websites maintained by the Plaintiffs are subject to overblocking. For example, www.powells.com, an online bookstore, was blocked at the domain level in its entirety by four of the filters, and certain pages were blocked by an additional four filters. All but two of the filters blocked, either entirely or partially, www.scarleteen.com, a web site operated by Heather Corrine Rearick that is apparently designed specifically for teenagers. In addition, www.sexualhealth.com, a sex education web site, was blocked either entirely or partially by every filter setting tested. (Mewett Testimony and Rebuttal Report ¶ 17)

146. Every Plaintiff has Web pages that are blocked by at least two filtering companies in categories designed to assist parents in protecting their children from inappropriate speech about sex. (Stipulations at ¶ 32)

147. In addition to the personal computer-based and ISP-based filtering products described above, certain search engines also offer filtering services with respect to searches performed on those search engines. Any user, however, can disable a search engine filter with

the click of a button; there is no password protection that would enable parents to ensure the filter is set at all times. (Mewett Testimony and Report ¶ 65)

148. Mr. Mewett tested filtering products offered by three search engines – Google, Yahoo!, and Verizon – by running the one hundred most popular search terms, as reported by Wordtracker, through those search engines. Even with the search engine filter setting activated, 3 percent of the top 100 Wordtracker queries returned sexually explicit web pages for Google; 8 percent returned sexually explicit web pages for Yahoo!; and 10 percent returned sexually explicit web pages for Verizon. This is a conservative test, because it is likely that search engine filters would focus their efforts on the most popular queries. (Mewett Testimony and Report ¶ 69)

149. Search engine filters face significant overblocking difficulties. For example, Google SafeSearch consistently blocks web sites operated by the U.S. government, by American newspapers, and by Fortune 1000 companies. Furthermore, Google SafeSearch frequently blocks even web sites that are specifically targeted at, or are helpful to, children. (Mewett Testimony and Report ¶ 79)

D. Large Portions of Domestically-Hosted Pornography Are Not Blocked by Filters

150. A substantial portion of the sexually explicit web pages that were not blocked by the filters are hosted in the United States. For the sets of web pages randomly drawn from the Google and MSN search engine indices, Dr. Stark's analysis found that between 31.6 percent and 49.7 percent of the sexually explicit and not-blocked web pages in that data set were hosted in the United States, varying by filter. (Stark Testimony)

151. These percentages generally increase for the web pages that were returned from a random sample of queries on the MSN, Yahoo!, and AOL search engines. Between 33.8 percent and 91.9 percent of the sexually explicit and not-blocked web pages in that data set were hosted in the United States, varying by filter. (Stark Testimony)

152. Those percentages increase further for the web pages that were returned from the most popular queries as reported by Wordtracker. Between 69.2 percent and 96.6 percent of the sexually explicit and unblocked web pages in that data set were hosted in the United States, varying by filter. (Stark Testimony)

153. Most sexually explicit web pages that are hosted outside of the United States have a commercial link to the United States. The vast majority of those web pages either directly solicit subscriptions or sales from their customers, including customers in the United States, or link to a web site that does so. Of the sexually explicit web pages in the data sets tested by Mr. Mewett that were hosted outside the United States, but that did not directly solicit subscriptions or sales, approximately 90 percent of those web pages either contained images that were themselves hosted in the United States, or linked to a web site that solicits subscriptions or sales. Specifically, 90.3 percent of the web pages in the Google index data set did so, 89.8 percent of the web pages in the MSN index data set did so, 88.2 percent of the web pages in the random search engine query data set did so, and 95.9 percent of the web pages in the Wordtracker query data set did so. (Stark Testimony and Rebuttal Report ¶ 26)

E. Other Problems with the Use (or Non-Use) of Filtering Software

154. The figures that are reported as the results of Mr. Mewett's and Dr. Stark's study reflect the likelihood that a filter, if installed and in proper working order, would block sexually

explicit material. However, not all users employ filters. Parents may choose not to use a filter because they find the software to be too restrictive, limiting the child's ability to research online effectively. (Mewett Testimony and Report ¶ 74)

155. A customer must have a significant degree of computer knowledge, and be willing to undertake a certain degree of effort, in order to install, configure, and update filters. An inexperienced parent is likely to face difficulties in installing the software or in attempting to remove it at a later date. Many computers are unable to effectively utilize filters due to technical constraints and compatibility problems, such as firewalls or anti-virus software. (Mewett Testimony and Report ¶ 74; Eisenach Testimony)

156. The conversion of residential households in the United States to broadband Internet connections will exacerbate the limitations of Internet content filtering software. Some personal computers will not be upgraded, but will be expected to cope with the increased volume of data made available at higher speeds through broadband connections. (Mewett Testimony and Report ¶ 74)

157. Internet content filtering software tends to be low-level software. The software is designed to install itself between the normal applications on a computer and the transport and protocol layers of the operating system's network communications. Software is not ordinarily installed at this level of the operating system. The potential therefore exists for the code of another program to conflict with the filtering software at this level, with adverse consequences for the entire operating system. (Mewett Testimony and Report ¶ 76)

158. Because filtering software generally is designed to be secure, any attempts to uninstall or reconfigure the software may be interpreted by the program as an attempt to

circumvent it. This could result in invalid configurations that will render the computer unusable or unable to connect to the Internet. (Mewett Testimony and Report ¶ 76)

159. Internet filters can be circumvented. There are many web sites available that describe how to disable or to circumvent specific filters, as well as filters in general. In some cases, it is possible to access these instructions even while the respective filter is turned on. For at least four of the filters that Mr. Mewett tested, he was able to obtain instructions from the Web on how to disable or bypass that filter, even with the filter turned on. For example, he was able to find a document at www.cexx.org/censware.htm outlining two methods for bypassing the Net Nanny filter by typing "disable net nanny parental controls" into the Google search engine with the Net Nanny filter on. (Mewett Testimony and Report ¶ 74)

160. Tech savvy teenagers, as well as anti-filtering activist groups, easily can circumvent filtering software through use of proxies, exploiting caches, software hacks, or backdoor passwords. For example, by typing in "getting around parental controls" into the Google search engine, the top two returns are instructions on how to bypass various filters. (Mewett Testimony)

161. Web proxy sites also can be used to gain access to Web sites that have been blocked. A proxy server allows clients to make indirect network connections to other network services. An example of a readily-available web site that instructs viewers on how to use proxy sites to circumvent filters is found at www.zensur.freerk.com. (Mewett Testimony and Report ¶ 74)

162. Translation tools may also be used to access sexually explicit Web sites in foreign languages. Sexually explicit search words may be typed in English into tools such as Google

translation, and the translated into a different language, resulting in a list of foreign URLs that likely can be accessed without being blocked by a filter. This is because most filtering is done through the use of English phrases. (Mewett Testimony and Report ¶ 74)

163. Some search engines use a technique called "cache," which permits a user to view a previous version of a web page if that page has changed after it is first found by the search engine's web crawler. Some filters may block a link to a particular web site with sexually explicit content, but would not block a cached image of that site. (Mewett Testimony and Report ¶ 74)

164. In addition to the many forms by which filtering software can be circumvented, pornography merchants also take steps to ensure that their websites will not be blocked. In particular, redirected URLs pose a difficulty for Internet content filtering software. Pornography merchants frequently acquire new or expired domains, with the intention of automatically forwarding the viewer of those domains to one or more of the merchants' own pornographic URLs. Pornography merchants have developed mechanisms through which hundreds of pornography URLs are rotated sequentially. (Mewett Testimony and Report ¶ 74)

165. Commercial pornography merchants also have stolen metatags from non-pornographic web sites. Because search engines use the metadata of a web page to determine the content of that page, the pornography merchants' use of this stolen metadata would prevent a search engine from identifying the page as sexually explicit, and may cause the search engine to direct a viewer to that site even if the viewer enters a search for non-pornographic material. (Mewett Testimony and Report ¶ 74)

166. No commercially-available products attempt to block web pages through an analysis of the images on the page. It is extremely difficult to identify images, or to categorize images as sexually explicit, through automated software. Home personal computers currently lack the capacity to support software that would have that capability. Since filtering software relies instead on analysis of words and phrases, a pornography merchant can evade the software by placing text on the website in the form of images. (Mewett Testimony and Report ¶ 74)

167. Many sexually explicit web pages do not use metatags, because the purveyors of those websites do not wish the sites to be identified by search engines as sexually explicit. (Mewett Testimony and Report ¶ 75)

168. Enterprise filtering software is more effective than residential filtering software. A corporate client would have the budget to employ the correct people to install and manage the filtering systems. In addition, the corporate client likely would want to ensure that its employees have access to only what is deemed to be necessary for productivity, and thus would wish to allow only a relatively small category of websites to be permitted, without concern about overblocking. In contrast, a parent is more likely to have a limited budget, limited knowledge, limited time, and non-standardized hardware and software. (Mewett Testimony and Report ¶ 72)

F. The Inherent Limitations of Filtering Software Technology

169. Filtering software relies on a formal analysis of the text of a web page to determine whether that page is sexually explicit. No automated system, however, is capable of analyzing the formal features of text with the accuracy needed to ensure that filtering software will be effective. (Neale Testimony)

170. These limitations of automated systems are inherent in any attempt to classify text on a purely formal basis. Thus, no text-based filtering system will ever be able to minimize both the underblocking of sexually explicit material and the overblocking of non-sexually explicit material. (Neale Testimony)

171. When configured to block access to sexually explicit material, filtering software blocks a substantial amount of material on the Web that is not sexually explicit or fails to block material that is sexually explicit. Filtering software is intrinsically unable to block sexually explicit material while simultaneously allowing minors access to all protected speech because all filtering involves an immutable trade-off between the overblocking caused by aggressive filter settings and the underblocking caused by more liberal settings. (Neale Testimony)

172. There is little reason to think the performance of filters or the basic principles of filtering will change in the foreseeable future because the problems are conceptual and linguistic. (Neale Testimony)

173. Filtering software is concerned with the problem of assigning Web pages to a set of predetermined categories. In this regard they are no different from systems and services that classify texts or images according to other properties, such as topic, genre, or type. (Neale Testimony)

174. Filters that rely solely on "black lists" cannot accurately capture all sexually explicit content. The effectiveness of filters, therefore, turns on the effectiveness of dynamic analysis of content. Dynamic filters must be able to detect and respond to features in Web pages that are considered indicative of content. For the most part, this means features of the text in

Web pages such as the presence of "keywords" and potentially revealing word distributions, which may be determined by statistical analyses. (Neale Testimony and Report)

175. Filtering software, like any other automated system, cannot understand the underlying content of text. It can only classify the formal features of text that it has been programmed to recognize, and perhaps weigh. The software uses these formal features of text to indicate the likely presence of the types of content humans would recognize and understand. But these formal features can never be a fully accurate proxy for the actual content of the text. (Neale Testimony and Report, ¶ 5.3.2)

176. No commercial filtering software exists that classifies Web pages by recognizing and weighing features of audio or video files. (Neale Testimony)

177. Image filtering is not effective. (Neale and Mewett Testimony)

178. Image-based classifiers/filters perform much worse than text-based classifiers/filters. Thus text-based classifiers form the core of current commercial filtering technology. To this extent, the effectiveness of current filtering software is largely a function of how well it manages to differentiate textual features and recognize connections among them. (Neale Testimony)

179. For the purposes of current text-filtering software, a text is nothing more than an unordered collection of words (and, in some cases, part words and near words) with no syntactic structure imposed upon them. So no difference is registered between, for example, "the dog chased the cat" and "the cat chased the dog," even if though the sentences have different meanings. (Neale Testimony)

180. No list of keywords (or key strings) can provide necessary and sufficient conditions for correct classification: words on any list can appear on Web pages that clearly should not be considered under a specified category; and pages that clearly should be classified as falling within a category need contain no word from that list. The more one expands the list so as to block more sexually explicit or pornographic sites, for example, the more one will overblock, *i.e.*, block non-explicit non-pornographic sites; and the more one contracts the list to reduce overblocking, the more one will underblock, *i.e.*, fail to block sexually explicit or pornographic sites. This relation between overblocking and underblocking is immutable. (Neale Testimony)

181. Classifying text without the means to assign phrase structure to it will not be effective. More sophisticated representations than unordered collections of words could be used by classification/filtering software, and it appears that some such software does use small numbers of short strings. But filtering software does not use, and, in light of the computational and comprehensional limits of filtering software, could never make use of anything like the sophistication of the structures that generative linguistics has discovered humans actually invoke in understanding the meaning of phrases or sentences. (Neale Testimony)

182. Automated systems are not currently able to replicate either the psychological complexity and creativity or the real world knowledge and perceptual, emotional, and social experience at the core of both the capacity to use and interpret language, and our capacity to understand the linguistic and non-linguistic behavior of one another. (Neale Testimony)

183. Computers are able to perform tasks that essentially consist of calculating probabilities and generally crunching numbers. What they cannot do, and will never be able to

do, is abstract features of sorts they have not been programmed to recognize, or form novel hypotheses about the world, or draw on a rich background of perceptual, emotional, and social experience that can be obtained only by living in the world and seeing how others with the same general physical and cognitive architecture live in it. (Neale Testimony)

184. No filtering products use "artificial intelligence," despite hyperbolic claims to the contrary. Filter companies refer to "neural nets" and "artificial intelligence" playing key roles in their statistical classifiers. However, while these references suggest a degree of "intelligence" that resembles or mimics human intelligence, understands patterns, or learns a language, such references are metaphorical only. (Neale Testimony)

G. Market Failure in the Filtering Software Industry

185. Filtering software is the only software that allows children to access the Internet while attempting to avoid inappropriate material. Filtering software can be somewhat effective, but only if parents actually use it. In fact, however, only a portion of households with minor children use filtering software. (Eisenach Testimony)

186. The potential market for home-based Internet content filtering software ("filtering software") is the 41 percent of Internet-connected households with children. (Eisenach Testimony)

187. Market survey evidence suggests that, most likely, approximately four out of ten of these Internet-connected households with children use filtering software. At most, 55 percent of these households do. (Eisenach Testimony and Principal Report ¶ 8)

188. This low level of penetration of filtering software into its potential market indicates a failure of the market to provide products which are effective and can be effectively

used by consumers. (Eisenach Testimony)

189. Families do not use filtering software for many reasons, including the following: (1) the burden and complexity of installing and using ICF software; (2) frustration with the under- and over-blocking of content; (3) the ability of children to circumvent ICF software; and (4) low demand for the product leave producers with little incentive to create and market a high-quality product. (Eisenach and Mewett Testimony)

190. The costs of using filtering software include the time parents must spend installing, setting up and maintaining the software, which for many parents, is a significant deterrent to filtering software use, and for some, an insurmountable one. (Eisenach Testimony and Principal Report ¶ 109)

191. Filtering software products are more difficult to use than other types of software. (Eisenach Testimony)

192. Parents are deterred from using filtering software because it causes over blocking and under blocking, and can be circumvented by children. (Eisenach Testimony and Principal Report ¶¶ 119-125)

193. The nature of the filtering software market is conducive to market failure because of the asymmetry of information between consumers and producers of the filtering software. (Eisenach Testimony)

194. The market for filtering software is smaller than the market for other kinds of security software, thereby causing filtering software producers to have weaker incentives to improve the quality of their product, and contributing to market failure. (Eisenach Testimony)

195. A market failure exists when the value to consumers of higher quality products, if

produced, would exceed the cost of producing them. (Eisenach Testimony)

196. Market analysis demonstrates that there will be an insignificant increase in home use of personal computer ICF software. (Eisenach Testimony)

197. There is a demand for good filtering products that is not being met. (Eisenach Testimony)

198. It is unlikely that better filtering software for home computers will be developed because the market is not large enough for the product. (Eisenach Testimony)

199. Filtering software producers lack an incentive to create a quality product because consumers make purchases without assessing the quality of the product. When consumers use the product, they are unable to determine whether the product is good or bad. Therefore, the filter market is stuck with no incentive to develop a better product. This is known as the "Lemon problem." (Eisenach Testimony)

200. In such markets, producers of high quality products are unable to obtain full value for the products they produce, since consumers are unable to distinguish high quality products from low quality products, and therefore are unwilling to pay the full cost of producing a higher quality product. (Eisenach Testimony and Principal Report ¶ 133; Def.'s Trial Ex. 29)

201. The market for filtering software products is such a market, and therefore the quality of filtering software is unlikely to improve significantly in the future. (Eisenach Testimony)

IV. COPA PROVIDES THE MOST EFFECTIVE SOLUTION TO THE PROBLEM

A. Credit Card Age Verification on the Web

202. Congress built several affirmative defenses into COPA to ensure that adults could

access material deemed harmful to minors, while restricting minors from such speech. It is an affirmative defense under COPA for a website to restrict access by minors to material that is harmful to minors by requiring the use of a "credit card, debit account, adult access code, or adult personal identification number," "by accepting a digital certificate that verifies age," or by "any other reasonable measures that are feasible under available technology." 47 U.S.C. § 231(c)(1).

203. It is an affirmative defense to prosecution under COPA to restrict, in good faith, access by minors to material that is harmful to minors by requiring use of a credit card. (Stipulations at ¶ 117)

204. It is an affirmative defense to prosecution under COPA to restrict, in good faith, access by minors to material that is harmful to minors by requiring use of a debit card, including a reloadable prepaid card. (Stipulations at ¶ 118)

205. "Traditional" payment cards refers to a credit card, debit card, and prepaid card (reloadable version only) issued by five card companies (*i.e.*, American Express, Diners Club, Discover, MasterCard, and Visa). Personal credit cards are essentially a loan from a financial institution to an individual or a company to make purchases with or obtain cash advances. Debit cards allow cardholders to access funds in their checking account to obtain cash and make purchases. Prepaid debit allows individuals to purchase a payment card and "pre-fund" it with cash or funds from one of their own credit cards and then use the prepaid debit card to obtain cash or make purchases (*e.g.*, gift cards, payroll cards, corporate incentive cards). (Clark Testimony)

206. "Traditional" payment cards (both credit and debit) are very popular and easy to

use. The near universal view is that credit and debit cards are "easy and convenient" to use. There are three primary reasons why the traditional payment cards are so popular: (1) there is no dollar liability for the consumer; (2) most consumers have established these cards as their primary payment vehicle; (3) these cards bring "guaranteed" business to the website operators. (Clark Testimony)

207. About 80% of U.S. consumers (*i.e.*, 18 years and older) have made purchases online. Since 2001, consumer comfort with Internet purchasing has increased significantly for both credit cards and debit cards. (Clark Testimony)

208. Currently, 66% of consumers feel "comfortable" or "completely comfortable" with using credit cards for online shopping and 50% feel comfortable with using debit cards. (Clark Testimony)

209. Both the Pew Internet & American Life Internet Project study Teens and Technology (July 27, 2005) and the Teenage Research Unlimited Spring 2006 wave 47 study found that about 37 percent of teens ages 12-17 had made purchases online. When 17-year-olds were excluded from the Teenage Research Unlimited data, the study found that only about 30 percent of teens ages 12-16 made online purchases. (Clark and Mann Testimony)

210. The Pew Internet & American Life study did not present any data that excluded 17-year-olds from their results, nor did it ask any questions or collect any data about how teens ages 12-17 paid for their online purchases. (Mann Testimony)

211. The Teenage Research Unlimited study found that about 60 percent of teens ages 12-17 who made online purchases used their parents' credit cards, about nine percent used their parents' debit card, and about two percent used a credit card in their name, but tied to their

parents' account. When 17-year-olds were excluded, the study found that about 60 percent of teens ages 12-16 who made online purchases used their parents' credit cards, about seven percent used their parents' debit card, and about 1.6 percent used their own credit card. (Mann Testimony)

212. Of the 73.6 million children under age 18 in the United States, only a few have payment cards. About 11% of children age 12-17 (25.5 million, U.S. Census), or 2.8 million children, have either a credit card or debit card. These payment cards are either an "extra" card on their parent's account or a "parent co-signed" card in the child's name. An additional 2.8 teens occasionally borrow their parents' credit cards to make occasional online purchases. (Clark Testimony)

213. In the United States, adult ownership of traditional payment cards is widespread and these cards are easy to use. However, this is not the case for children, since card issuers have always been reluctant to issue accounts to individuals under 18 due to state laws. (Clark Testimony)

214. Parents of minor children who borrow their parent's payment cards to make online purchases can ask their children what they are going to purchase. (Stipulations at ¶ 99)

215. Each state has a law that defines the "age of majority." That is the age when an individual who enters into a contract can not be released from the commitment due to age. This is important to the financial institution to ensure that they can collect an outstanding balance (*e.g.*, credit card, debit card tied to a checking). Most states set the "age of majority" at 18. Five states have the age set higher than 18 (*e.g.*, Alabama 19, Indiana 21, Nebraska 21, New Hampshire 21, Pennsylvania 21). Further, some states allow individuals under 18 years old to be

considered "age of majority" individuals under special circumstances (*e.g.*, Utah, any age if married). (Clark Testimony)

216. Most adults own either a credit card (*e.g.*, American Express, Discover, MasterCard, Visa) or a debit card tied to their checking account (*e.g.*, Discover, MasterCard, Visa). However, even "unbanked" adults can acquire and use reloadable prepaid cards to make purchases on the Web. Pursuant to the requirements of the Know Your Customer Provisions of the USA Patriot Act, issuing banks require a purchaser of a reloadable prepaid card to be an adult. (Clark Testimony)

217. Prepaid debit cards, also known as prepaid cards and stored-value cards, include "closed" system cards (such as store gift cards, cell-phone cards, or transit cards that are accepted by one specific merchant), and "open" system cards that are accepted by many merchants. Some cards are single purpose or non-reloadable, and some are reloadable. The cards can be used to purchase goods/services and access cash at ATMs. A consumer can purchase and load these cards at a bank or retailer, over the phone or online. Usually there is a fee of $5-$8 per card; generally these cards are available in amounts up to $500. For reloadable cards, the Patriot Act requires that the card issuer collect certain information as part of the Patriot Act's "know your customer" provision (*e.g.*, name, address, phone number, birth date). Based on the most recent data, "open" system cards represent less than 0.8 percent of the dollar volume in payment cards. (Clark Testimony)

218. The emergence of (non-reloadable) prepaid gift cards is not an obstacle to limiting children's access to harmful-to-minors material. If a Web merchant cannot successfully perform the two operational verifications now common for most online transactions (*i.e.*, billing

address and CVC, the three digit number on the back of a payment card), the website operator is likely to decline that transaction. Since non-reloadable gift cards do not have a billing address and present a higher degree fraud risk, website operators can and generally will decline to accept these (non-reloadable) prepaid gift cards. Indeed, payment processors for commercial adult sexual content websites do not generally accept gift cards (non-reloadable prepaid cards). On the other hand, reloadable prepaid cards have billing addresses due to the Patriot Act "know your customer" provision and therefore generally will be accepted by website operators. (Clark Testimony)

219. Parents can supervise their children's online transactions at the time of purchase. However, even if actual purchases made with these cards are unsupervised, parents can see their children's payment card purchases online two to three days after the purchase is made, and, in some cases, the same day. (Clark Testimony)

220. Commercial website operators that offer adult sexual content can process a zero-dollar transaction or charge a membership/access fee, but either transaction will appear on the card billing statement and allow the parent to supervise their children. Virtually all adult cardholders are familiar with reviewing a billing statement, and with calling the card issuer to inquire about unfamiliar or suspect purchases. Parents can thus monitor their children's online purchasing behavior. (Clark Testimony)

221. Although the growth of non-reloadable prepaid "gift" cards has been rapid, the vast majority of the growth has been with the "closed-system" products, such a Sears Gift Card. The size of "open-system" products, such as the Visa Gift Card, is minimal. (Clark Testimony)

222. The two primary Internet Payment Service Providers that control the adult

entertainment market, CCBill.com and Paycom.net, require a billing address in order to purchase access to online adult entertainment. Non-reloadable prepaid cards do not have a billing address. (Clark Testimony)

223. In general, over 95% of commercial website operators in the U.S. accept traditional payment cards. (Clark Testimony)

B. Micro-Payment Technology Facilitates the Purchase of Content

224. Bitpass was founded in 2002 to provide solutions that remove the roadblocks to digital content commerce and to allow digital media and entertainment companies to cash in on their content assets. Today producers and aggregators of digital media may want higher returns from investments in content. At the same time, rapidly changing consumer buying and usage behaviors may be redefining the digital media marketplace. Bitpass connects digital media producers with this growing market, offering solutions that increase return on content, customers and community. (Knopper Testimony)

225. The Bitpass iMedia Commerce Engine marshals relevant delivery channels—including the web, cell phones, PDAs, MP3 players, podcasts and other digital media devices. (Knopper Testimony)

226. The Bitpass iMedia Commerce Engine offers digital media and entertainment companies a turnkey system built on open web standards and a software-as-a-service platform. The iMedia Commerce Engine supports rapid deployment, transparent web and commerce integration and secure financial transactions, consumer behavior tracking and seamless content and data integration. (Knopper Testimony)

227. Bitpass customers include leaders from media publishing, TV, film, radio,

community and Internet and include segment leading firms such as Disney, Microsoft and MSN, Ziff Davis, Time, United Media, CanWest, and Entercom. (Knopper Testimony)

228. The iMedia Commerce Engine is available as an enterprise system or a self-service solution. Both products have access to the payment, security, fulfillment and analytics services of a high-availability technology platform. (Knopper Testimony)

229. Consumers use iMedia Account to purchase and access digital content on iMedia merchant sites. iMedia Account is a digital wallet application that offers consumers "frictionless" purchasing and complete privacy and anonymity. (Knopper Testimony)

230. iMedia Account is a "digital wallet" for the web. Consumers enter payment card, PayPal information, add some money the account and get single click purchasing. Consumers spend what is in the wallet and iMedia Account lets them know when they need to add more money. (Knopper Testimony)

231. Consumers pay with the funds in the account not the payment card information, which stays safe with Bitpass. iMedia does not require consumers to disclose personal information every time they make a purchase. (Knopper Testimony)

232. The iMedia Account has features for consumers to manage their accounts. Consumers can set purchase thresholds and track funding, purchases, log-in sessions and complaints and refunds. iMedia accounts are free to set up, have no monthly fees, and can be funded with as little as $3. (Knopper Testimony)

233. Products such at Bitpass make the process of purchasing online content simple and convenient, without interrupting a website visitor's experience with the "flow" of the website. Purchases can be as little as $0.99, $0.10, or even for free. (Knopper Testimony)

234. Bitpass is ready to offer a version of its product to merchants that only accept Bitpass accounts tied to a payment card. Bitpass is developing a product that allows parents to monitor their children's Bitpass activity. (Knopper Testimony)

235. Bitpass is considering developing a product that would allow consumers to "purchase" content for free by watching a video advertisement. Such purchases will still require a Bitpass account and there will be a record of the purchase. (Knopper Testimony)

C. Online Age Verification Services Are Highly Effective

236. Age verification services can prevent minors from accessing harmful content. (Dancu Testimony and Dillon Testimony)

237. One technologically feasible manner in which websites can screen for age is through age verification services ("AVS products" or "AVS technologies"). AVS products, which currently are used for online wine and tobacco sales, require a consumer to enter personal information—usually their name, address, and the last four digits of their Social Security number. The information is then verified using commercially available databases that aggregate public records. The process is completed in less than a second. (Dancu Testimony and Dillon Testimony)

238. The AVS products generate questions based on personal historical information, such as the color of a given car or the address of a previous home. AVS companies tailor these quiz products to meet the needs of their consumers. Obviously, the more questions that are asked, the more effective the verification process. (Dancu Testimony and Dillon Testimony)

239. AVS products are sophisticated enough to ensure that a customer is not using someone else's personal information. (Dancu Testimony and Dillon Testimony)

240. Age verification can be completed at little cost, which can be absorbed by the website operator. The cost, which currently ranges from as little as 25 cents to as much as $1.00, depending on the volume of transactions and the websites' tolerance level for errors, will drop dramatically when there is a high volume of transactions. An age verification password can be issued to certify that a consumer is not a minor and can be reused over a specified period of time on the same or different websites. (Dancu Testimony and Dillon Testimony)

241. In addition to the commonly used methods of age verification, some promising "digital wallet" technologies are on the horizon, which can make online identity verification even easier than face-to-face verification, such as Microsoft's InfoCard. (Dancu Testimony)

242. Digital certificates are now technologically viable and are used by at least one bank. (Dillon Testimony)

243. Although age verification products are the most reliable existing method, the options for online identity and age verification are becoming more numerous, more effective, and increasingly inexpensive to implement. (Dancu and Dillon Testimony)

D. Implementation of COPA Will Not Materially Affect the Web

1. Businesses Can Adapt to a Minor Regulatory Change in the Adult Entertainment Industry

244. COPA will have no significant negative impact on commercial websites on the Internet. (Smith Testimony)

245. The Internet is a stable, established business communications tool, and COPA will not require the creation of a new business model. COPA will have no negative effect on commercial innovation or business models used in Internet commerce. (Smith Testimony)

246. Requiring the use of a payment card before website visitors can access adult

sexual content on these websites places almost no burden on these merchants (apart from the potential costs of web redesign to segregate such content). Those few commercial website operators who publish adult sexual content but do not accept payment cards can select from three alternative approaches to process payment cards: (1) setup their own merchant account for traditional card payments; (2) use third party merchant account for traditional card payments; or (3) offer non-traditional payment vehicles like PayPal. The costs to honor the traditional payment cards are modest (generally between 2.5% to 5.5% of sales dollar volume), and even lower for PayPal. These costs, fraud and processing fees, are likely to decline over the next three to five years. (Clark Testimony)

247. Requiring the use of a payment card to view such content "monetizes" a product that is in high demand. Requiring the use of a payment card likely will deter only those visitors who were unlikely to make a purchase, and thus unlikely to affect business results. (Clark Testimony)

248. On the other hand, Bitpass offers its merchant customers the option of "selling" its content to consumers for free (usually at some cost to the merchant), and is developing a product that allows customers to "purchase" content by watching a 30- or 60-second video advertisement. In either case, however, the transaction creates a payment record that the parents can review. (Knopper Declaration and Testimony)

2. Consumers Are Adaptable and Increasingly Willing to Provide Personal Information on the Internet

249. Internet commerce is thriving, which suggests that consumers are becoming increasingly comfortable with providing personal information on the Internet. (Smith Testimony)

250. Consumers are increasingly willing to register or provide a credit card in order to gain access to websites. (Smith Testimony)

251. COPA will not inhibit qualified consumers from viewing online content. COPA's qualification standards, which require a password, registration or a purchase, are used successfully in many businesses where controlled products and services are purchased and consumed. (Smith Testimony)

252. Barriers are common in successful everyday shopping activities on the Internet. COPA's regulation of access to certain content by minors under the age of 17 will have no significant adverse effect on adults who access, search for information, or use the Internet. (Smith Testimony)

253. The modest burdens associated with COPA's affirmative defenses are analogous to the burdens associated with obtaining access to adult material in other settings, such as entries to nightclubs, adult bookstores, or NC-17 movies. (Smith Testimony)

254. Visually consumed products are traditionally paid for prior to consumption. Consumers pay in advance to see movies, Broadway plays or musical, art museum tours, and even national parks. Consumers expect to pay the required fee for visually consumed products prior to consumption. Because COPA requires qualification by methods other than credit card use, the merchant retains the option to not require purchase before a consumer views content. (Smith Testimony).

255. Consumers are willing to tolerate economic barriers in the form of time, inconvenience, or money to achieve a goal. From an economic perspective, this inelasticity of demand may be high where loyalty to a product is high, or where the consumer derives sufficient

value from the product. (Smith Testimony)

256. The pornography industry traditionally has faced both social and technological barriers that have not reduced industry demand. Every time a new medium for the dissemination of pornography is created, the technological advances have required not only a shift in consumer use behavior, but a shift in the business model within the industry. Yet there has not been a decrease in demand for the product category. (Smith Testimony)

257. The consumption of pornography requires a motivated user, one who actively seeks access to website pornography. The minimal qualification standards required by COPA are smaller than the barriers required to consume pornography through any other medium because the purchase can be made in the privacy of one's home. (Smith Testimony)

258. Visitors intending to purchase are not likely to be deterred by entering a payment card at the entry screen because they are likely to still see the same benefits as before, such as convenience and anonymity. (Clark Testimony)

259. Moreover, requiring the use of a payment card should lead to repeat visits to the website where the website visitor has "registered" a payment card and/or obtained a membership for automatic access in the future. Thus, requiring the use of payment card should improve revenue levels. (Clark Testimony)

260. The Better Business Bureau and the Javelin Strategy & Research issued the 2005 Javelin Identity Fraud Survey Report. A summary of that report noted that: (1) the most frequent reported source of information used to commit fraud was a lost or stolen wallet or checkbook; (2) among cases where the perpetrator's identity is known, half of all identity fraud is committed by a friend, family member, relative, neighbor, or in-home employee; and (3) a wide variety of

metrics confirm that identity fraud problems are not worsening, with the total number of victims in decline. (Clark and Smith Testimony)

3. Commercial Websites Easily Can Comply with COPA

261. There is no technical obstacle that would prevent commercial adult porn sites from utilizing one or more of the screening mechanisms set out in COPA for limiting access to harmful to minors material. (Clark and Smith Testimony; Dillon and Dancu Testimony)

262. Some commercial adult porn sites do block all access to materials on their site unless and until a valid credit card or other form of adult identification (including adult password) is supplied; however, many adult porn sites, numbering in the thousands, voluntarily choose to provide access to free sample images and texts. (H.R. Rep. No. 105-775, at 10; Russo Testimony)

263. COPA's affirmative defenses reflect Congress's understanding of the business model of commercial pornography to present "teasers" to garner business, and Congress's desire to ensure that the adult content is not contained in such publicly-accessible "teasers," but is restricted to the audience for which it is intended – adults. Congress noted that the affirmative defenses already "represent standard procedures for conducting commercial activity on pornographic Web sites," and that the affirmative defenses simply ensure that "the commercial pornographer . . . put sexually explicit images 'behind the counter.'" (H.R. REP. NO. 105-775, at 15)

264. COPA's affirmative defenses are technologically feasible and readily available to commercial pornographers. Even though they are not covered by COPA, the Plaintiffs in this litigation would have no difficulty restricting access to content by minors. Indeed, most of the

Plaintiffs currently accept payment cards or link to second-party sellers who do. (Plaintiffs' Testimony and Stipulations at ¶¶ 100-09)

E. COPA Provides a Worldwide Solution

265. COPA applies equally to operators of both foreign and domestic web sites. COPA applies to anyone who "knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors . . ." 47 U.S.C. § 231(a)(1). Congress did not limit COPA's application on the basis of the residency of the website operator or the geographic location of the server hosting the website.

266. The United States has entered into more than fifty bilateral Mutual Legal Assistance Treaties (MLATs) with other countries. These agreements provide the United States with the power, in investigating a violation of its laws that may have been committed by a resident of another country, to request the assistance of a signatory country to summon witnesses, to compel the production of evidence, to issue search warrants, and to serve process. *See, e.g.*, Treaty Doc. 105-12, 105th Cong., 1st Sess., Exec. Rpt. 105-22, 105th Cong., 2d Sess. (U.S.-Poland MLAT).

267. BetonSports PLC, a company organized under the laws of the United Kingdom; David Carruthers, its chief executive officer; ten other persons; and three other entities were indicted by a grand jury in the United States District Court for the Eastern District of Missouri on June 1, 2006. The indictment charges several offenses, including the violation of 18 U.S.C. § 1804 for the transmission of wagers. In response to the indictment, the board of directors of

BetonSports PLC announced that it would suspend its United States Internet wagering operations, which were physically based in Costa Rica and Antigua. (Def.'s Trial Ex. 80)

268. Each of the card companies (e.g., Amex, Discover, MasterCard, Visa) have worldwide policies, operating rules and agreements, which govern any retailer or website operator worldwide that accepts payment cards. These agreements require compliance with all applicable laws and regulations. Further, if a website operator fails to comply with any applicable law, then the card companies can take one of several actions to correct this: impose increasingly severe fines and/or entirely rescind the right of the website operator to accept that company's payment card. (Clark Testimony)

269. Merchant agreements require foreign merchants selling goods and services to U.S. customers to comply with laws that are unique to the United States. For example, the card companies have required merchants to comply with important compliance regulations such as the Fair Credit Billing Act and the Truth & Lending Act. Thus, once COPA is in effect, foreign providers of commercial pornography will be required to satisfy COPA's regulatory requirements or risk fines or rescission of their right to accept cards. (Clark Testimony)

270. Recently, non-profit business and law enforcement communities announced the organization of the Financial Coalition Against Child Pornography. The Coalition, coordinated by two non-profit groups that focus on preventing child exploitation, brought together card companies, card processing companies, banks, and Internet companies such as AOL, American Express, Chase, Citigroup Discover, First Data MasterCard, Visa, and Wells Fargo to set up a CyberTipline to identify website operators that sell child pornography, cut off their use of payment cards, and share this information with law enforcement communities. By identifying

website operators that do not restrict access to adult sexual content, cutting off their use of payment cards, and sharing this information with law enforcement communities, the payment industry and law enforcement can target international commercial websites just as easily as domestic ones. (Clark Testimony)

271. Adapting the Financial Coalition Against Child Pornography to include COPA would essentially be a "fine tuning" process (*e.g.*, adding appropriate other non-profit agencies, adding appropriate new members, as well as adjusting operating tactics to focus also on commercial website operators that provide adult sexual content). The net result would be that children's access to adult sexual content (adult sex acts and content) would be targeted for control and enforcement. (Clark Testimony)

272. Founded in January 2000, Quova, Inc. is the authority on intellectual property Intelligence and the leading provider of IP geolocation data and services to online businesses, including five of the world's six largest global Internet companies. Quova's patented technology provides the geographic location of website visitors in real time, enabling businesses to detect fraud, manage digital rights, target content, conduct site analysis and ensure regulatory compliance. Quova's customers and partners include such industry leaders as Major League Baseball Advanced Media, BBC, Bell Canada, Cisco Systems, Coremetrics, Corillian, PassMark, Bankinter, Globo, Times Online and Sky Sports. (Alexander Testimony)

273. Quova is used to comply with FFIEC guidance, the Office of Foreign Assets Control (OFAC) regulations, the USA PATRIOT Act, and the Bank Secrecy Act, each of which have made knowing the location of online bank and credit union customers more important than ever. Quova is also used by the pharmaceutical, software, and online gaming industries, each of

which are subject to regulations restricting where they can offer their products and services. (Alexander Testimony)

274. Quova can be used for content localization to customize website content to reflect the cultural preferences and priorities of online visitors from different regions and different countries. (Alexander and Connor Testimony)

V. THERE ARE NO VIABLE ALTERNATIVES TO COPA

A. Inadequacy of Voluntary Solutions

275. Other potential alternatives to COPA will not be as effective in protecting minors from exposure to sexually explicit material on the World Wide Web. The creation of separate and voluntary top-level domains for adult material, or for material designated as child-friendly, will not prevent minors from being exposed to sexually explicit material on the World Wide Web. Self-segregation on the Internet will accomplish little beyond increasing the use of the keyboard's "x" key, again underscoring the need for a *mandatory* solution that regulates harmful material *at its source*. (Russo Testimony)

276. According to Marv Johnson, legislative council for the ACLU, the creation of a "dot-xxx" top-level domain name is "not going to make a whole lot of difference" in stopping minors from finding pornography. (http://www.physorg.com/news12015.html) (Stipulations at ¶ 98)

277. Top-level domains must be established by the Internet Corporation for Assigned Names and Numbers ("ICANN"), an independent international organization. ICANN rejected a proposal to create a ".xxx" domain. Even if a ".xxx" domain were created, in order to be effective it must be mandatory and backed up with penalties for non-compliance. (Russo

Testimony; Def.'s Trial Ex. 381)

278. A separate child-friendly Internet domain will not prevent the conveyance of harmful material to children. There is no need to speculate on the effectiveness of having a child-friendly Internet domain, because Congress authorized a second-level domain in 2002, *see* 47 U.S.C. § 941, and NeuStar administers a top-level ".kids" domain. (http://www.neustar.biz/addressing/kidsDom.cfm and http://www.kids.us/)

279. The top-level domain name "www.kids.us" contained a trivial number of websites, thus guaranteeing that children will be unable to complete even basic homework tasks without accessing the traditional domains on the Web. (Allen Testimony)

B. Government Has Exhausted Alternative Means

280. Recognizing that COPA is not a substitute for filters, and that COPA can work in conjunction with private filtering that parents may utilize, COPA amended a section of the Communications Act of 1934 to require providers of Internet services to notify customers, at the time the customer signs up for services, that parental control protections, such as computer hardware, software, or filtering services, are commercially available to assist the customer in limiting access to material that is harmful to minors. 47 U.S.C. § 230(d). (See Stipulations at ¶ 120)

281. Since the passage of COPA, Congress has enacted additional laws regulating the Internet in an attempt to protect minors. For example, it has enacted a prohibition on misleading Internet domain names, 18 U.S.C. § 2252B, in order to prevent Web site owners from disguising pornographic Web sites in a way likely to cause uninterested persons to visit them.

282. Congress recently passed a law prohibiting the misleading use of metatags to

entice viewers to view material on pornographic websites. 18 U.S.C. § 2252C.

283. Congress also passed legislation that mandates the use of filtering programs in public schools and libraries that receive funds under two popular federal programs. (Stipulations at ¶ 120) (*See United States v. American Library Ass'n, Inc.*, 593 U.S. 194, 203 n.2 (2003)) (finding that the government can condition receipt of federal funds on public libraries' use of filters and declaring Children's Internet Protection Act constitutional).

284. Congress passed a law providing funding to "Children's Safety Online Awareness Campaigns." The legislation allows the Attorney General "to develop and carry out a public awareness campaign to demonstrate, explain, and encourage children, parents, and community leaders to better protect children when such children are on the Internet." Pub. L. No. 109-248, 120 Stat. 587 (July 27, 2006).

285. None of these initiatives can be fully successful in preventing minors from viewing sexually explicit content. Despite these initiatives, the rate at which minors are exposed to sexually explicit material on the Web has continued to increase. (Finkelhor Testimony)

PROPOSED CONCLUSIONS OF LAW

I. SUMMARY OF COPA

1. COPA's objective is to prevent commercial pornography websites from offering minors access to the material on their sites. H.R. Rep. No. 105-775, at 15 (1998). To that end, COPA establishes criminal and civil penalties when a person "knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors." 47 U.S.C. § 231(a)(1)-(3).

2. A person communicates "for commercial purposes" only if he "is engaged in the business of making such communications," 47 U.S.C § 231(e)(2)(A), and a person is engaged in the business of making such communications only if he "devotes time, attention, or labor" to making harmful-to-minors communications "as a regular course of [his] trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income)." *Id.* at § 231(e)(2)(B).

3. COPA applies only to persons who seek to profit from placing harmful-to-minors material on their websites as a regular course of business. 47 U.S.C. § 231(a)(1), (e)(2). This narrow tailoring distinguishes COPA from the Communications Decency Act, which the Supreme Court found to be overbroad. *ACLU*, 521 U.S. at 879.

4. Only a person who "knowingly causes the material that is harmful to minors to be posted on the World Wide Web or knowingly solicits such material to be posted on the World Wide Web" will be considered to be "engaged in the business of making, by means of the World Wide Web, communications for commercial purposes that include material that is harmful to minors." 47 U.S.C. § 231(e)(2)(B).

5. COPA does not apply to Internet access service providers (commonly referred to as "ISPs," such as America Online or Cox Communications) or Internet information location tool providers. 47 U.S.C. § 231(b)(2)-(3). An Internet information location tool is "a service that refers or links users to an online location on the World Wide Web. Such term includes directories, indices, references, pointers, and hypertext links." *Id*. at § 231(e)(5). In addition, COPA does not apply to those "similarly engaged in the transmission, storage, retrieval, hosting,

formatting, or translation . . . of a communication made by another person, without selection or alteration of the content of the communication." *Id*. at § 231(b)(4).

6. COPA defines "material that is harmful to minors" as "any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind" that is "obscene" or that:

> (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;
>
> (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
>
> (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

47 U.S.C. § 231(e)(6).

7. COPA defines a minor as "any person under 17 years of age." *Id.* at § 231(e)(7). This narrow tailoring distinguishes COPA from the Communications Decency Act, which the Supreme Court found to be overbroad. *ACLU*, 521 U.S. at 879.

8. COPA provides "an affirmative defense to prosecution" if a person, "in good faith, has restricted access by minors to material that is harmful to minors." 47 U.S.C. § 231(c)(1). A person qualifies for this affirmative defense by (A) "requiring use of a credit card, debit account, adult access code, or adult personal identification number," (B) "accepting a digital certificate that verifies age," or (C) taking "any other reasonable measures that are feasible under available technology." *Id.* Information collected for the purpose of restricting

minors' access to materials covered by the Act is protected from unauthorized disclosure. *Id*. at § 231(d).

II. PLAINTIFFS LACK STANDING

A. Website Plaintiffs Lack Standing

9. None of the Plaintiffs has standing to maintain this action. In order to maintain standing, a party must show that he has sustained or is immediately in danger of sustaining some direct injury due to the challenged conduct and this injury or threat of injury must be real and immediate, not conjectural or hypothetical. *City of Los Angeles v. Lyons*, 461 U.S. 95, 101-02 (1983).

10. Plaintiffs cannot maintain standing for their vagueness claim (Count Four). In the Third Circuit, "a vagueness attack requires the plaintiff to show that he himself was injured by the vague language of the regulation." *Gibson v. Mayor & Council of Wilmington*, 355 F.3d 215, 225-26 (3d Cir. 2004).

11. Allegations of subjective chill do not suffice to maintain standing. *Laird v. Tatum*, 408 U.S. 1, 13-14 (1972); *Aiello v. City of Wilmington*, 623 F.2d 845, 857 (3d Cir. 1980); *Am. Library Ass'n v. Barr*, 956 F.2d 1178, 1194 (D.C. Cir. 1992).

12. None of the Plaintiffs has a credible fear of prosecution under COPA. Because Plaintiffs' alleged fear of prosecution is based on a subjective chill, rather than objective evidence, they lack standing to challenge the constitutionality of COPA.

13. Established precedent from state harmful-to-minors laws that contain definitions similar to COPA provides guidance as to the scope of harmful-to-minors material under COPA. *See, e.g., See Reno v. ACLU*, 521 U.S. 844, 887 n.2 (1997) (listing state "harmful to minors"

statutes) (O'Connor, J., concurring in part and dissenting in part); *Ginsberg v. State of New York*, 390 U.S. 629 (1968); *Am. Booksellers Ass'n v. Virginia*, 882 F.2d 125, 127 (4th Cir. 1989); *Athenaco, Ltd. v. Cox*, 335 F. Supp. 2d 773, 781-82 (E.D. Mich. 2004).

14. None of the objective evidence submitted by Plaintiffs supports their alleged fear of prosecution because none of the examples proffered by Plaintiffs comes within COPA's definition of "harmful to minors."

15. A court or jury is unlikely to find beyond a reasonable doubt that any of Plaintiffs' websites violate COPA. A court or jury is unlikely to find beyond a reasonable doubt that Plaintiffs' web pages violate COPA because they are not designed to appeal to, or designed to pander to, the prurient interest of minors. For example, Sexual Health Network posts a response to a question about how to deal with a child who is caught having sexual relations with a dog. This web page, although dealing with a sexual theme, is not designed to appeal to the prurient interest. (Def.'s Trial Ex. 283, No. 11).

16. Plaintiffs' websites do not contain material that is "lewd" and "patently offensive with respect to minors," or that otherwise "lack[] serious literary, artistic, political, or scientific value for minors." Plaintiffs' websites contain, *inter alia*, scientific sexual education information, literary content, artistic content, and political content. For example, Sexual Health Network, Scarleteen, and Condomania provide valuable scientific information regarding sexual education. Other websites, such as Femmerotic and Nerve, show photographs with artistic value. Still others, such as Scarlet Letters, Salon, and Wildcat International evidence serious literary value for minors. (Def.'s Trial Ex. 283, Nos. 11-14).

B. Associational Plaintiffs Lack Standing

17. An association has standing to sue on behalf of its members when: (a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit. *Hunt v. Washington State Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977).

18. Associational plaintiffs ACLU, ABFFE and EFF have not demonstrated standing on behalf of their members.

19. Associational plaintiffs ACLU, ABFFE and EFF have not demonstrated that their members would have standing to sue in their own right. *Hunt v. Washington State Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977).

20. Associational plaintiffs ACLU, ABFFE and EFF do not have standing because the claims asserted in this case require the individual participation of individual members in the lawsuit. *Hunt v. Washington State Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977).

C. Listener Plaintiffs Lack Standing

21. Plaintiffs have not produced evidence sufficient to state a claim on behalf of so-called "listener" Plaintiffs. Any listener Plaintiffs should have come forward with evidence to prove their standing, and cannot rest on the allegations of the Complaint, which formed the basis of the Court's original decision. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) (party asserting jurisdiction needs to prove it at each stage of litigation); *McNutt v. General Motors Acceptance Corp.*, 298 U.S. 178, 189 (1936) (plaintiff must support standing by "competent proof" when standing is challenged).

III. JUDGMENT SHOULD BE GRANTED TO DEFENDANT ON COUNT TWO OF THE AMENDED COMPLAINT

22. Plaintiffs' second cause of action fails because there is no constitutional right for older minors to access harmful-to-minors material. *See Bellotti v. Baird*, 443 U.S. 622, 634 (1979) ("the constitutional rights of children cannot be equated with those of adults"); *Ginsberg*, 390 U.S. 629, 638 ("[E]ven when there is an invasion of protected freedoms the power of the state to control the conduct of children reaches beyond the scope of its authority over adults") (internal quotations omitted); *Sable Comm'n of Cal., Inc. v. FCC*, 492 U.S. 115, 126 (1989) (finding that government has "a compelling interest in protecting the physical and psychological well-being of minors" and that "[t]his interest extends to shielding minors from the influence of literature that is not obscene by adult standards").

23. Minors' access to harmful-to-minors material may be constitutionally restricted. Under the *Ginsberg* concept of "variable obscenity," material deemed harmful to minors is unprotected as to minors. *Ginsberg v. New York*, 390 U.S. 629, 638 (1968); *see also M.S. News Co. v. Casado*, 721 F.2d 1281, 1289 (10th Cir. 1983).

24. Plaintiffs' second cause of action must fail because COPA does not restrict older minors' access to material appropriate for older minors. *See, e.g., Am. Booksellers v. Webb*, 919 F.2d 1493, 1504-05 (11th Cir. 1990) (in construing a statute defining minors as under 18 years old, concluding that "if any reasonable minor, including a seventeen-year-old, would find serious value, the material is not 'harmful to minors'"); *Am. Booksellers Ass'n v. Virginia*, 882 F.2d 125, 127 (4th Cir. 1989) ("if a work is found to have a serious literary, artistic, political, or scientific value for a legitimate minority of normal, older adolescents, then it cannot be said to lack such value for the entire class of juveniles taken as a whole") (quoting *Virginia v. Am. Booksellers*

Ass'n, 732 S.E.2d 618, 624 (Va. 1988)); *Davis-Kidd Booksellers, Inc. v. McWherter*, 866 S.W.2d 520, 533 (Tenn. 1993) (finding material has serious value for minors within the meaning of that State's display law, if it has serious value for "a reasonable seventeen year old minor").

IV. JUDGMENT SHOULD BE ENTERED FOR DEFENDANT ON COUNT THREE OF THE AMENDED COMPLAINT

25. There is no constitutional right to access material anonymously on the Web. While the Supreme Court has recognized a right to anonymous speech in certain circumstances, this line of cases is inapposite to the instant case because COPA does not entail public disclosure of anyone's identity or require identification to any government officials. *See Buckley v. Am. Constitutional Law Found.*, 525 U.S. 182 (1999) (striking down statute requiring volunteers to wear identification badges); *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995) (allowing anonymous pamphleteering on political issues); *Talley v. Calif.*, 362 U.S. 60 (1960) (finding First Amendment to protect distribution of unsigned handbills urging the boycott of merchants); *Lamont v. Postmaster Gen.*, 381 U.S. 301, 305 (1965) (striking down law requiring recipients of "communist political propaganda" through mail to perform an "official act," that is, to affirmatively request that post office deliver material).

26. Courts have upheld laws intended to restrict access by minors to sexually explicit material, even if such laws may require adults who desire such material to affirmatively request it or to identify themselves in some manner. *See Crawford v. Lungren*, 96 F.3d 380, 387-89 (9th Cir. 1996) (upholding constitutionality of law regulating sale of "harmful to minors" material in vending machines which allowed access by adults who could verify their adulthood); *Information Providers' Coalition for Defense of First Amendment v. FCC*, 928 F.2d 866, 872-74 (9th Cir. 1991) (upholding credit card or adult access code requirement in the "dial-a-porn"

context); *Doe v. City of Minneapolis*, 693 F. Supp. 774, 783 (D. Minn. 1988) (finding no First Amendment right to anonymously view sexually explicit material in bookstore booths), *aff'd*, 898 F.2d 612 (8th Cir. 1990); *Upper Midwest Booksellers Ass'n v. Minneapolis*, 780 F.2d 1389, 1395 (8th Cir. 1986) (upholding constitutionality of display restriction in part because "[a]dults are still free to request a copy of restricted material to view from a merchant").

27. Plaintiffs' third cause of action must fail because Plaintiffs do not have a right to communicate or access harmful-to-minors content anonymously. *Cf. Connection Distributing Co. v. Reno*, 154 F.3d 281 (6th Cir. 1998) (rejecting anonymity claims raised by "swingers" magazine); *Fabulous Assoc., Inc. v. Pennsylvania Public Utility Comm'n*, 896 F.2d 780, 788 (3d Cir. 1990) (suggested dial-a-porn regulation that required customers to identify themselves to telephone companies in order to unblock access to services is constitutionally permissible where "there is evidence that the telephone company will not disclose such information"); *Crawford v. Lungren*, 96 F.3d 380, 387-89 (9th Cir. 1996) (upholding constitutionality of law regulating sale of "harmful to minors" material in vending machines which allowed access by adults who could verify their adulthood); *Information Providers' Coalition for Defense of First Amendment v. FCC*, 928 F.2d 866, 872-74 (9th Cir. 1991) (upholding credit card or adult access code requirement in the "dial-a-porn" context); *Doe v. City of Minneapolis*, 693 F. Supp. 774, 783 (D. Minn. 1988) (finding no First Amendment right to anonymously view sexually explicit material in bookstore booths), *aff'd*, 898 F.2d 612 (8th Cir. 1990); *Upper Midwest Booksellers Ass'n v. Minneapolis*, 780 F.2d 1389, 1395 (8th Cir. 1986) (upholding constitutionality of display restriction in part because "[a]dults are still free to request a copy of restricted material to view from a merchant").

28. Absent consent or a court order, COPA prohibits the disclosure of "any information collected for the purposes of restricting access to such communications to individuals 17 years of age of older." 47 U.S.C. § 231(d)(1)(A). Further, the statute requires that a company that verifies the age of an adult who accesses harmful to minors material to "take such actions as are necessary to prevent unauthorized access to such information by a person other than the [company] and the [adult]." *Id.* at § 231(d)(1)(B). Anyone who willfully or knowingly violates these provisions is subject to criminal penalties. *See* 47 U.S.C. § 501.

29. COPA's inclusion of a non-disclosure prohibition renders Plaintiffs' contention that their speech or access to speech will be restricted because of loss of anonymity a constitutionally insignificant contention. *See Connection Distrib. Co. v. Reno*, 154 F.3d 281, 294 (6th Cir. 1998); *Fabulous Assoc., Inc. v. Penn. Public Utility Comm'n*, 896 F.2d 780, 788 (3d Cir. 1990). Moreover, any harm Plaintiffs claim as a result of the purported infringement on their anonymous access is speculative. *See California Bankers Ass'n v. Schultz*, 416 U.S. 21, 55 (1974).

V. JUDGMENT SHOULD BE ENTERED FOR DEFENDANT ON PLAINTIFFS' FIRST AMENDMENT OVERBREADTH CLAIM

A. Intermediate Scrutiny Should Be Applied

30. The statutory text and legislative history demonstrate that COPA applies to commercial speech. COPA regulates only "communication[s] for commercial purposes," 47 U.S.C. § 231(a)(1), and "person[s] engaged in the business of making such communications." *Id.* at § 231(e)(2)(A). As Congress noted when it passed COPA, pornography on the Internet is inherently commercial in nature, and free teasers are used to entice a consumer into making a commercial transaction. S. Rep. No. 105-225, at 1-2 (1998).

31. Some commercial pornography websites propose a commercial transaction directly to the consumer on their own site, while others do so through advertisements on affiliated sites. The latter are so-called "feeder websites." COPA regulates the advertising on both types of websites because both business models make "communication[s] for commercial purposes." 47 U.S.C. § 231(a)(1).

32. COPA does not reach non-commercial speech, even on the World Wide Web. 47 U.S.C. § 231(a)(1); (e)(2)(A). (Stipulations ¶ 119)

33. Because COPA regulates commercial speech, such as the content of "free teasers" and "feeder websites" that serve as advertisements for the enticement of a subsequent sale, it should be reviewed using intermediate scrutiny. Laws regulating commercial speech are permissible if the government has a "substantial interest" that is directly advanced by "narrowly drawn" regulation. *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y.*, 447 U.S. 557, 564-65 (1980). In other words, there must be a "reasonable fit" between the statute's ends and the means chosen to accomplish those ends. *Florida Bar v. Went For It, Inc.*, 515 U.S. 618, 632 (1995).

34. COPA easily satisfies this test. As shown below, Defendant has not only a substantial interest, but a compelling one, in protecting minors from exposure to sexually explicit material on the World Wide Web. COPA will help protect minors to a material degree: there is a reasonable fit between Congress's ends in enacting COPA and the commercial pornography that it regulates.

35. An overbreadth challenge cannot be sustained against a statute regulating commercial speech. *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489,

497 (1982) (stating that "the overbreadth doctrine does not apply to commercial speech"). Plaintiffs therefore may bring a facial challenge to COPA only if the statute has no possible constitutional application. COPA certainly has many constitutional applications.

B. COPA Satisfies Even Strict Scrutiny

1. Legal Standards

36. Even if the Court considers COPA to be a content-based restriction for which strict scrutiny applies, Defendant is able to meet his burden. In such a situation, the statute at issue "must be narrowly tailored to promote a compelling Government interest" to be constitutional under the First Amendment. *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803, 813 (2000).

37. If strict scrutiny were to apply to COPA, in order to succeed on their overbreadth challenge, Plaintiffs must demonstrate that "no set of circumstances exists under which the Act would be valid." *United States v. Salerno*, 481 U.S.739, 745 (1987), or that COPA is "substantially overbroad." *New York State Club Ass'n v. City of New York*, 487 U.S. 1, 11 (1988). "The overbreadth claimant bears the burden of demonstrating, from the text of [the law] and from actual fact," that substantial overbreadth exists." *Virginia v. Hicks*, 123 S. Ct. 2191, 2197 (2003).

38. Plaintiffs have failed to meet their burden of showing that COPA has no constitutional applications or is "substantially overbroad." *See New York v. Ferber*, 458 U.S. 747, 769 n.24 (1982).

39. For a law to be unconstitutionally overbroad, its impermissible applications must be "'substantial,' not only in an absolute sense, but also relative to the scope of the law's plainly

legitimate applications." *Virginia v. Hicks*, 123 S. Ct. 2191, 2197 (2003).

40. The Court will invalidate a statute as facially overbroad only as a last resort and only if the Act has a substantial number of impermissible applications. *United States v. Knox*, 32 F.3d 733, 751-52, 771 (3d Cir. 1994).

41. The Supreme Court has noted that facial challenges are "to be discouraged," and it has "recognized the validity of facial attacks alleging overbreadth . . . in relatively few settings, and, generally on the strength of specific reasons weighty enough to overcome our well-founded reticence." *Sabri v. United States*, 541 U.S. 600, 609-10 (2004).

42. The Court will construe the statute to avoid constitutional problems if the statute is subject to a limiting construction. *New York v. Ferber*, 458 U.S. 747, 769 (1982).

2. The Government Has a Compelling Interest in Protecting Minors

43. The Defendant has a compelling interest in protecting minors from exposure to sexually explicit material on the World Wide Web. The Supreme Court has firmly established that the government has "a compelling interest in protecting the physical and psychological well-being of children" and that "[t]his interest extends to shielding minors from the influence of literature that is not obscene by adult standards." *Sable Comm'n of Cal., Inc. v. FCC*, 492 U.S. 115, 126 (1989). *See also Reno v. ACLU*, 521 U.S. 844, 864-65 (1997); *Ginsburg v. New York*, 390 U.S. 629, 639 (1968).

44. There are two components to the compelling government interest in the protection of minors. The government has an interest in aiding parents who wish to protect their children from the harmful effects of pornographic material. *Reno v. ACLU*, 521 U.S. 844, 865 (1997). In addition, the government has an independent interest in the well being of the nation's minors.

Id.

45. COPA does not restrict minors' rights to obtain any constitutionally protected materials. Under the *Ginsberg* concept of "variable obscenity," material deemed harmful to minors is unprotected as to minors. *Ginsberg v. New York*, 390 U.S. 629, 638 (1968); *see also M.S. News Co. v. Casado*, 721 F.2d 1281, 1289 (10th Cir. 1983). Minors' access to such material, accordingly, may be constitutionally restricted.

46. Plaintiffs' contention that COPA fails to effectively serve the government's compelling interest is unsupported by evidence and cannot serve as the basis for finding the Act facially invalid.

3. COPA Is Narrowly Tailored

47. COPA's definition of "harmful to minors," found at 47 U.S.C. § 231(e)(6), is directly derived from the tests for obscenity as to minors developed by the Supreme Court in *Miller v. California*, 413 U.S. 15 (1973), and *Ginsberg v. New York*, 390 U.S. 629 (1968) and patterned after the narrowly interpreted state harmful-to-minors statutes with harmful-to-minors definitions that have been upheld by numerous courts. H.R. Rep. No. 105-775, at 27-28 (1998).

48. As the decisional law surrounding the regulation of obscenity-related speech makes evident, the harmful-to-minors standard employed in COPA reaches only materials that are clearly pornographic and inappropriate for minors. COPA does not apply to materials that merely contain nudity or profanity or that merely espouse controversial political or sexual viewpoints, as those materials would not fall within the established definition of "harmful to minors" adopted by COPA. *See* H.R. Rep. No. 105-775, at 28; *see also Osborne v. Ohio*, 495 U.S. 103, 112 (1990); *New York v. Ferber*, 458 U.S. 747, 765 n.18 (1982); *Board of Education v.*

Pico, 457 U.S. 853 (1982); *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 214 n.10 (1975); *Jenkins v. Georgia*, 418 U.S. 153, 161 (1974).

49. In drafting COPA, Congress addressed the specific concerns raised by the Supreme Court to ensure the law would be narrowly tailored. COPA applies only to material posted on the World Wide Web, where age screening is both technologically feasible and affordable. 47 U.S.C. § 231(a)(1); H.R. Rep. No. 775 at 13-14. This narrow tailoring distinguishes COPA from the Communications Decency Act, which the Supreme Court found to be overbroad. *ACLU*, 521 U.S. at 879.

50. COPA defines minors as those under the age of 17, an age distinction that the Supreme Court has upheld in the harmful-to-minors context. 47 U.S.C. § 231(e)(7). *Ginsberg v. N.Y.*, 390 U.S. 629 (1968).

51. COPA's definition of "harmful to minors" contains three prongs, each of which must be met in order for materials to be deemed "harmful to minors." 47 U.S.C. § 231(e)(6).

52. The first prong of COPA's harmful-to-minors definition is that the material must be designed to appeal or pander to the prurient interests. 47 U.S.C. § 231(e)(6)(A). This requires that material be designed to appeal or pander to a morbid or shameful interest in sex or nudity. *Brockett v. Spokane Arcades, Inc.*, 472 U.S. 491, 498 (1985).

53. The second prong of COPA's harmful-to-minors definition limits the scope of "harmful to minors" materials to those that depict or describe specific conduct (actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast) in a patently offensive manner with respect to minors. 47 U.S.C. § 231(e)(6)(B). Courts have indicated that these limitations

are to be narrowly construed. *Osborne*, 495 U.S. at 113; *Erznoznik*, 422 U.S. at 214. This narrow tailoring distinguishes COPA from the Communications Decency Act, which the Supreme Court found to be unconstitutional. *ACLU*, 521 U.S. at 879.

54. The third prong of COPA's harmful-to-minors definition is that the material must lack serious literary, artistic, political or scientific value for minors. 47 U.S.C. § 231(e)(6)(C).

55. If material has serious value for older minors, it will be considered to have value for all minors. *See, e.g., Am. Booksellers v. Webb*, 919 F.2d 1493, 1504-05 (11th Cir. 1990) (in construing a statute defining minors as under 18 years old, concluding that "if any reasonable minor, including a seventeen-year-old would find serious value, the material is not harmful to minors"); *Am. Booksellers Ass'n v. Virginia*, 882 F.2d 125, 127 (4th Cir. 1989) ("if a work is found to have a serious literary, artistic, political, or scientific value for a legitimate minority of normal, older adolescents, then it cannot be said to lack value for the entire class of juveniles taken as a whole") (quoting *Virginia v. Am. Booksellers Ass'n*, 732 S.E.2d 618, 624 (Va. 1988)); *Davis-Kidd Booksellers, Inc. v. McWherter*, 866 S.W.2d 520, 533 (Tenn. 1993) (finding material has serious value for minors within the meaning of that State's display law, if it has serious value for "a reasonable seventeen year old minor").

56. Both the first and third prong of COPA's harmful-to-minors definition require that the material be judged "as a whole." In *Kois v. Wisconsin*, the Court held that the "as a whole" language requires a "reviewing court [to] look at the context of material, as well as its content." 408 U.S. 229, 231 (1972). This contextual analysis has been a mainstay of obscenity law since *Roth* was decided in the 1950s. *See Kois*, 408 U.S. at 231 (holding that, even if particular photographs in a newspaper would be obscene "by themselves," they could not be the

basis for an obscenity prosecution where, "in the context in which they appeared in the newspaper they were rationally related to an article that itself was clearly [not obscene]"); *Roth v. United States*, 354 U.S. 476, 490 (1957) (requiring examination of "entire context" of books, pictures and circulars alleged to be obscene).

57. Websites are analogous to magazines, in which individual pictures or articles are examined in the context of the entire magazine. *Manual Enterprises, Inc. v. Day*, 370 U.S. 478, 489 (1962); *Ginzburg v. United States*, 383 U.S. 463, 466 n.5 (1966). Several Plaintiffs, such as Salon, Nerve and Philadelphia Gay News, are online magazines or newspapers.

58. Because COPA does not apply to hosting entities, Plaintiffs' concerns regarding both the content of Web sites to which they provide links, and materials that are posted on their sites by persons other than themselves through the various Web-based interactive fora they purport to include on their sites are invalid and unwarranted. 47 U.S.C. § 231(b)(4).

59. COPA does not ban or significantly restrict protected speech by adults. The requirement that COPA-regulated speech be placed behind an age-verification "curtain" is no more restrictive than state-law display requirements that require harmful-to-minors speech to be physically segregated, placed behind blinder racks, or accessed only by a token or other device intended to verify adult access. *See Crawford v. Lungren*, 96 F.3d 380 (9th Cir. 1996); *American Booksellers v. Webb*, 919 F.2d 1493 (11th Cir. 1990); *Upper Midwest Booksellers Ass'n v. City of Minneapolis*, 780 F.2d 1389 (8th Cir. 1986); *M.S. News Co. v. Casado*, 721 F.2d 1281 (10th Cir. 1983). COPA is akin to an electronic brown paper wrapper and, accordingly, is constitutional.

60. COPA does not "ban" online communications that are harmful to minors.

Instead, COPA regulates only the manner in which such communications can be displayed so as to restrict minors' access to them.

61. The Supreme Court has repeatedly held that Congress has authority to enact laws that are narrowly tailored to protect minors from harmful material. *Reno v. ACLU*, 521 U.S. at 864-865; *Sable*, 492 U.S. at 126; *Ginsberg*, 390 U.S. at 639. That authority necessarily includes the power to place reasonable burdens on adults when it is necessary to protect minors from harmful material. *See Am. Library Ass'n*, 123 S. Ct. 2297, 2307 (2003). Any other rule would strip Congress of the ability to vindicate that compelling interest.

62. Congress borrowed from a solid foundation of cases upholding similar measures in formulating a structure that places the burden on the information content provider to restrict access to harmful-to-minors communications, rather than on the parent or child to avoid those communications. *See Dial Information Servs. v. Thornburgh*, 938 F.2d 1535 (2d Cir. 1991) (citing *Sable Communications of California, Inc. v. FCC*, 429 U.S. 115 (1989)); *Information Providers' Coalition for Defense of the First Amendment v. FCC*, 928 F.2d 866 (9th Cir. 1991). Such a scheme is clearly constitutional.

63. COPA's narrow tailoring does not undermine its effectiveness because most commercial pornography is "accessible, over the Internet, using hypertext transfer protocol or any successor protocol," thus placing such material within COPA's definition of communications "by means of the World Wide Web." 47 U.S.C. § 231(e)(1). Even if, for example, commercial pornographers were to shift to use the FTP protocol, any future use of FTP as a means to transmit commercial pornography would, by any practical definition, constitute a "successor" protocol to HTTP and would be regulated by COPA.

64. Further, any commercial pornography that is placed on the Internet through the FTP protocol, but that is "publicly accessible" by the viewer through the use of HTTP, is covered by COPA. Because it is virtually certain that commercial pornographers would continue to use HTTP for at least some purposes, their content will continue to be regulated by COPA.

65. Even if some forms of pornography were unregulated, nothing prevents Congress from choosing to regulate an industry incrementally. *United States v. Edge Broadcasting Co.*, 509 U.S. 418, 427-29 (1993).

66. COPA effectively serves the government's compelling interest in protecting minors from sexually explicit content on the World Wide Web. Its limitation to content placed on the Web for commercial purposes does not impair its effectiveness, as the vast majority of such adult content has a commercial purpose. The Web poses particular dangers of inadvertent exposure, and ready access, of minors to harmful-to-minors materials.

67. Before the Supreme Court in *Reno v. ACLU*, Plaintiff ACLU successfully argued that the Communications Decency Act was unconstitutionally overbroad, in part because it applied both to non-commercial speech as well as commercial speech, and also in part because it applied to e-mail, chat rooms, newsgroups, and other forms of communication on the Internet beside the World Wide Web. Br. of Appellees, *Reno v. ACLU*, No. 96-511, at 28-29 (filed Feb. 20, 1997) (available at 1997 WL 74738). Plaintiffs cannot reverse course and argue that COPA will be effective only if it regulates a broader range of speech, and if it regulates other forms of communication.

4. COPA Is the Most Effective Way to Prevent Minors from Accessing Harmful Material

a. Viability of Affirmative Defenses

68. COPA provides affirmative defenses to prosecution that are feasible and not burdensome. 47 U.S.C. § 231(c)(1)(A)–(C). COPA will be effective in protecting minors from exposure to sexually explicit material on the World Wide Web.

69. Age verification technologies are not only technologically available but are used by commercial providers of sexually explicit materials.

70. Website operators easily can comply with COPA. The placement of harmful-to-minors material behind a credit card screen is a valid affirmative defense under the statute. 47 U.S.C. § 231(c)(1)(A). Credit cards are widely used on the World Wide Web, their use on the Web is easy to implement, and their use would ensure that only adults would have access to material behind the credit card screen. Online purchases made by those few children that have access to payment cards can easily and effectively be supervised by their parents.

71. Congress reasonably listed credit cards as an affirmative defense to COPA. Congress noted that credit cards are an affirmative defense in the FCC's dial-a-porn regulations, which has been upheld by the courts. *See* H.R. Rep. 105-775 at 14 (citing *Dial Info. Serv's Corp. v. Thornburgh*, 938 F.2d 1535 (2d Cir. 1991), *cert. denied*, 502 U.S. 1072 (1992), and *Sable*, 429 U.S. 115 (1989)).

72. Congress also took note of the Supreme Court's approval of affirmative defenses (such as credit cards) within laws protecting minors from sexually explicit material when it stated, "the FCC's technological approach to restricting dial-a-porn messages to adults who seek them would be extremely effective, and only a few of the most enterprising and disobedient

young people would manage to secure access to such messages." H.R. Rep. 105-775, at 14 (quoting *Sable*, 429 U.S. at 130).

73. Even if using credit cards would place an economic burden on commercial websites, such a burden does not render COPA unconstitutional, as "there is no constitutional impediment to enacting a law which may impose costs on a medium electing to provide [indecent] messages." *Sable*, 492 U.S. at 125. *See also Mitchell v. Comm'n on Adult Entertainment Establishments*, 10 F.3d 123, 144 (3d Cir. 1993) (when availability of adult content is not significantly impaired, law's effect on plaintiff's revenue is not material to First Amendment analysis); *Matney v. County of Kenosha*, 86 F.3d 692, 700 (7th Cir. 1996) ("The fact that [the ordinance] may have an incidental financial effect on adult entertainment speakers and not on others is of no consequence."). Those few commercial websites operators that publish adult sexual content but do not yet accept credit or debit cards can utilize one of COPA's other affirmative defenses.

74. Other technologies exist that will allow website operators to ensure that only adults would have access to harmful-to-minors material on their websites. For example, technology exists to permit website operators to process "micro-payments," and that technology can be used, in conjunction with a payment card transaction, to restrict minors' access to harmful-to-minors material. 47 U.S.C. § 231(c)(1)(A).

75. In addition, there are effective age verification services that are available for a website operator to use to ensure that only adults have access to his or her website, or to portions of his or her website. These services constitute "reasonable measures that are feasible under

available technology" to "restrict[] access by minors to material that is harmful to minors." 47 U.S.C. § 231(c)(1)(C).

76. COPA's age verification measures would be effective in excluding most juveniles, and "only a few of the most enterprising and disobedient young people would manage to secure access." (H.R. Rep. No. 105-775, at 14 (quoting *Sable Communications of Cal. v. FCC*, 492 U.S. 115, 130 (1989)).

b. COPA Provides a Worldwide Solution

77. COPA applies equally to operators of both foreign and domestic web sites. COPA applies to anyone who "knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors . . ." 47 U.S.C. § 231(a)(1). Congress did not limit COPA's application on the basis of the residency of the website operator or the geographic location of the server hosting the website. The statute is replete with references to the World Wide Web and Internet—terms which by definition have no geographic limitation. For example, the Internet is defined as the "combination of computer facilities and electromagnetic transmission media . . . comprising the interconnected worldwide network of computer networks . . ." *Id.* at § 231(e)(3).

78. Under established law, courts have jurisdiction to enforce COPA against foreign website operators. The Third Circuit has applied other pornography-related statutes abroad when the goal is to "contain the evils caused on American soil by foreign as well as domestic suppliers" of pornography. *United States v. Harvey*, 2 F.3d 1318, 1327 (3d Cir. 1993) (internal citation omitted); *see also United States v. Thomas*, 893 F.2d 1066 (9th Cir. 1990), *cert. denied*,

498 U.S. 826 (1990) (same).

79. COPA would be effective in protecting minors from exposure to sexually explicit material on the World Wide Web, whether that material is produced in the United States or in other countries. A significant portion of that material is found on websites hosted in the United States, and the most popular pornography is disproportionately found within the United States. Nonetheless, United States laws governing the Internet can be directly enforced even against operators of websites that are hosted abroad. In fact, the foreign-based BetonSports was recently indicted for violating United States law. (Def.'s Trial Ex. 80).

80. COPA also can be enforced abroad indirectly through the payment card industry's enforcement of terms in payment agreements. The payment card industry can require foreign producers of sexually explicit material who make that material available to minors in the United States over the World Wide Web to comply with United States laws. The vast majority of commercial pornography has commercial links to the United States. In the unlikely event that the payment card industry does not voluntary comply with United States law, nothing prevents Congress from enacting legislation to ensure that COPA is enforced by the industry worldwide. *See United States v. Edge Broadcasting Co.*, 509 U.S. 418, 427-29 (1993) (stating that Congress may choose to regulate an industry incrementally).

5. There Are No Less Restrictive Alternatives to COPA

a. The Private Use of Filtering Software Cannot Be Deemed a Less Restrictive Alternative for the Government

81. The ineffectiveness of filtering software, in addition to its limited use, leaves a significant gap in the collective effort to protect minors—a gap that the government can fill through enforcement of COPA. Filtering software will continue to exist, and will continue to be

available for use by families, whether or not Defendant is permitted to enforce COPA.

82. The enforcement of COPA, accompanied by the availability of filtering software for private use, provides a more effective means of protecting children than such filtering alone.

83. The private use of filtering software cannot be deemed a "less restrictive alternative" for the purpose of constitutional analysis. The proper inquiry is whether alternatives available to the *government* "would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve." *Ashcroft v. ACLU*, 542 U.S. 656, 665 (2004) (quoting *Reno v. ACLU*, 521 U.S. 844, 874 (1997)).

b. The Promotion of Voluntary Efforts Is Not an Effective Way to Protect Children from the Exposure to Harmful Material

84. Voluntary measures such as a website rating system, filtering products, and education, will be effective only if they are used in conjunction with the requirements of COPA, because voluntary measures alone will not prevent children from accessing material harmful to minors.

85. The establishment of a voluntary website rating system would be ineffective because website operators would lack an incentive to label their material in a manner that makes it more likely that filters will block access to the website. The operators would have to agree to a uniform system of ratings, or agree to subject themselves to an independent rating body for "binding" ratings.

86. The use of a government "black list," in addition to raising many of the same (or more) constitutional objections present here, would be ineffective for the same reasons that blacklists are ineffective when used with filtering software. Websites are too numerous and change too frequently for the government, or any private business, to effectively separate

harmful from non-harmful material. Only a solution directed at the source of the problem can provide the incentive necessary to adequately protect children.

87. Requiring filtering products to create a "harmful to minors" category would not be effective because that alternative assumes that filters are widely used, and that they prevent minors from accessing harmful content. Moreover, such an alternative would be effective only if companies were *required* to block access to certain sites.

88. User-based restrictions like voluntary filtering will not be as effective as COPA's requirements and are inconsistent with Congress's judgment that any burdens associated with restricting minors' access to harmful to minors materials pursuant to COPA should be placed on the source of such materials. Plaintiffs cannot demonstrate, therefore, that the less restrictive alternatives they propose are equally able to accomplish the Act's goals. *See Dial Information Servs. v. Thornburgh*, 938 F.2d 1535, 1542 (2d Cir. 1991).

c. Educational Efforts Will Not Be as Effective as COPA in Protecting Children from the Exposure to Harmful Material

89. Plaintiffs assert that the government could "promote media literacy and Internet safety education." Compl. at 11 ¶ 9. This cannot be deemed a less restrictive alternative for at least two reasons. First, the government is already pursuing these goals. *See* Pub. L. No. 109-248, 120 Stat. 587 (July 27, 2006). Second, this theory assumes that parents, when properly educated by the government, invariably can protect their children from the harmful material lurking on the World Wide Web. This argument fails because parents are unable to prevent accidental viewings of such materials, and the widespread availability of the Web subverts parental control.

90. Voluntary efforts by parents to monitor their children's Internet usage, or to educate their children about sexually explicit material on the World Wide Web, will not prevent minors from being exposed to such material.

d. Obscenity Prosecutions Are Not a Less Restrictive Alternative, Because COPA Applies to a Broader Category of Speech than Obscenity

91. An increase in obscenity prosecutions will not prevent minors from being exposed to sexually explicit material on the World Wide Web, because the scope of "harmful to minors" material is broader than the "obscene" material. Unlike criminal obscenity laws, however, COPA does not ban any material. It merely requires that consumers of harmful-to-minors material provide verification.

92. Material is obscene, under the standard set forth in *Miller v. California*, 413 U.S. 15 (1973), if (a) an average person applying contemporary community standards finds that the material taken as a whole appeals to the prurient interest; (b) an average person applying contemporary community standards finds that the material depicts sexual conduct in a patently offensive manner; and (c) a reasonable person, viewing the material as a whole, finds that the material lacks serious literary, artistic, political or scientific value. *See id.* at 24.

93. Examples of websites that have been prosecuted as obscene include, *inter alia*, child pornography, depictions of bondage and sadistic or masochistic behavior involving children, sexual contact between an adult woman and a dog, violent gang rapes of women, sexual intercourse between humans and animals, and sexual activity involving urination, defecation, or genital mutilation. (Def.'s Trial Ex. 283, No. 18).

94. Obscenity law regulates a very narrow category of speech that is entitled to no

First Amendment protection, while COPA has broader application, creating a category of regulated material that is obscene for minors, not adults. *Ashcroft v. ACLU*, 542 U.S. 656, 675 (Stevens, J., concurring).

95. The "harmful to minors" standard used in COPA differs from the *Miller* test in two respects. First, it requires that each prong of the *Miller* test be analyzed with respect to older minors. In addition, the second prong of the harmful-to-minors standard provides a more detailed description of material that a judge or jury may find to be "patently offensive" than the *Miller* obscenity test. 47 U.S.C. § 231(e)(6)(B).

96. The *Miller* test provides a standard that is judged by reference to the reasonable adult, whereas COPA provides a standard with respect to older minors. *See Am. Booksellers v.* Webb, 919 F.2d 1493, 1506 (11th Cir. 1990). Because COPA regulates harmful material beyond that which adults find obscene, its effects cannot be replicated by other criminal statutes. *See ACLU*, 521 U.S. at 875 (noting a "governmental interest in protecting children from harmful materials" that do not meet the court's definition of obscenity for adults).

97. Obscenity laws provide no protection for minors from harmful-to-minors material that is not obscene.

98. Even the most graphic photographs submitted on April 17, 2006 by Plaintiffs from Penthouse.com—depictions of full female nudity—are unlikely to be deemed to rise to the level of obscenity. Although this material may satisfy COPA's definition of "patently offensive" with respect to minors (e.g., there is a graphic and lewd focus on the genitals), it is unlikely to be deemed patently offensive under the *Miller* test with respect to adults. (Def.'s Trial Ex. 283, No. 16). Enforcement of COPA is necessary in order to prevent minors from accessing material

like the pages from Penthouse.com.

e. The Misleading Domain Names Statute Is Not a Panacea

99. The Misleading Domain Names statute cannot be considered a less restrictive alternative because it is already in existence; it has been in effect for three years. 18 U.S.C. § 2252B. In fact, the rate at which minors are exposed to sexually explicit material on the Web has continued to increase since this Act was passed.

100. The Misleading Domain Names statute is not as effective as COPA because it applies only to websites that entice visitors to a website by deceptive means. 18 U.S.C. § 2252B. The statute does not address websites that are, by name or reputation, indisputably pornographic. It applies only to instances in which a domain name is typed directly into a browser, and thus does not protect minors from exposure to harmful-to-minors websites that are accessed by other means. Further, the statute does not require that harmful-to-minors material be made accessible only after a website visitor proves his or her age.

f. Plaintiffs' Suggestions for Narrowing the Application of COPA Would Undermine Its Effectiveness

101. Plaintiffs' proposals for a "more limited, more narrowly tailored statute," *see* Pls.' Disputed Facts, pp. 65-68 (Doc. No. 319), would undermine the effectiveness of COPA (e.g., permitting only civil penalties for non-compliance and applying COPA only to images). COPA applies a constitutionally-approved standard for variable obscenity. It is well-established that the government has a compelling interest in protecting minors from harmful-to-minors material, and that category is not limited to images alone.

102. Moreover, because of the profitability of the commercial pornography industry, civil penalties alone will not suffice.

VI. JUDGMENT SHOULD BE ENTERED FOR DEFENDANT ON PLAINTIFFS' FIRST AMENDMENT VAGUENESS CLAIM

103. To survive a vagueness challenge, criminal statutes "need only give 'fair warning' that certain conduct is prohibited." *San Filippo v. Bongiovanni*, 961 F.2d 1125, 1136 (3d Cir. 1992). A vagueness challenge is particularly difficult to sustain because COPA does not apply to entities that unknowingly make harmful to minors material available to minors by means of the World Wide Web. *See* 47 U.S.C. § 231(a)(1), (e)(2)(B).

104. Case law has narrowed and sharply defined material that can be regulated in order to protect children. *See, e.g.*, *Am. Booksellers Ass'n*, 372 S.E.2d at 622 & 625 (finding that sixteen books, including Judy Blume's *Forever*, *Hollywood Wives, Changing Bodies, Changing Lives* and *Our Bodies Ourselves*, had serious literary, artistic, political or scientific value for minors); *Athenaco, Ltd. v. Cox*, 335 F. Supp. 2d 773, 781 (E.D. Mich. 2004) (finding works including *Lolita*, *Sanctuary*, *Of Mice and Men*, *The Catcher in the Rye*, *Portnoy's Complaint*, and *Joy of Sex* not to be harmful to minors); *Baker v. Glover*, 776 F. Supp. 1511, 1516 (N.D. Ala. 1990) (finding bumper sticker with phrase "Eat Shit" not to be harmful to minors).

105. The language of COPA gives fair warning about the regulated conduct covered by the statute. 47 U.S.C. § 231(e)(6). Mere nudity is not enough to render material harmful to minors. *See Osborne v. Ohio*, 495 U.S. 103, 112 (1990) ("depictions of nudity, without more, constitute protected expression"); *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 213 n.10 (1975) ("It is clear . . . that under any test of obscenity as to minors not all nudity would be proscribed. Rather, to be obscene 'such expression must be, in some significant way, erotic.'") (quoting *Cohen v. California*, 403 U.S. 15, 20 (1971)). In *Osborne*, the Supreme Court upheld a state obscenity regulation where the term nudity was construed to require "a graphic focus on the

genitals." *Osborne*, 495 U.S. at 113. COPA incorporates this standard within the second prong and also defines the specific types of actions that must be present in a patently offensive manner. *See* H.R. Rep. 105-775 at 13, 28 (noting that COPA "modifies the 'patently offensive' language by explicitly describing material that is harmful to minors" and that "harmful to minors" test does not extend to "materials that merely contain nudity").

106. There is a clear difference between material posted on Plaintiffs' websites and the type of material that Defendant has identified as likely to be deemed "harmful to minors." COPA does not apply to entities that unknowingly make harmful to minors material available to minors by means of the World Wide Web. *See* 47 U.S.C. § 231(a)(1), (e)(2)(B).

107. Material that Defendant has found likely to be deemed harmful to minors contains lewd depictions of full-frontal nudity in its free content area, including a photograph of a woman exposing her labia and clitoris and a photograph of a woman turned to her side, spreading her buttocks, and revealing her vagina and anus. This opinion was based on the conclusion that this material is designed to appeal to, or designed to pander to, the prurient interest and will likely be found to be patently offensive with respect to minors, and that a court or jury likely would find that they do not have serious literary, artistic, political, or scientific value for minors. (Def.'s Trial Ex. 283, No. 15).

108. Defendant opined in discovery that websites contain mere nudity (such as certain images provided to Defendant from the Playboy.com website) are not likely to be deemed harmful to minors. Although one web page identified by Plaintiffs on April 17, 2006 from Playboy.com contains one photograph depicting female breasts, the majority of the pictures do not contain any nudity, and there is no depiction of sexual activity or full frontal nudity. These

specific photographs from the Playboy.com website do not explicitly depict sexual acts or graphically focus on the genitals. (Def.'s Trial Ex. 283, No. 15).

109. In determining whether a given work has value, the proper inquiry is "whether a reasonable person would find such value in the material, taken as a whole." *Pope v. Illinois*, 481 U.S. 497, 501 (1987). It is important to note that the value of a work does not "vary from community to community based on the degree of local acceptance it has won." *Id.* at 500. Because this prong is not judged by community standards, but, instead, sets a "national floor" of societal value, *see Reno*, 521 U.S. at 873, Plaintiffs' speculative fears that the harmful-to-minors test will by applied in vastly different ways by different communities is unavailing.

110. The *Miller* and *Ginsberg* standards repeatedly have been upheld over vagueness challenges. *See, e.g., Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46, 57 (1989).

111. Judgment should be entered for Defendant.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

PATRICK L. MEEHAN
United States Attorney
RICHARD BERNSTEIN
Assistant U.S. Attorney
THEODORE C. HIRT
Assistant Branch Director
RAPHAEL GOMEZ
Senior Trial Attorney

/s/ Eric J. Beane
ERIC J. BEANE
ISAAC CAMPBELL
JOEL McELVAIN
KENNETH SEALLS
JAMES TODD

TAMARA ULRICH
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W.
Washington, DC 20530
(202) 616-2035

Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that on October 9, 2006, I caused the foregoing Proposed Findings of Fact and Conclusions of Law to be filed electronically and therefore to be available for viewing and downloading from the Electronic Case Filing system. The electronic filing of this document constituted service of this document on the following liaison counsel:

Aden Fine
American Civil Liberties Union
125 Broad Street, 18th Floor
New York, NY 10004

/s/ Eric J. Beane
ERIC J. BEANE